PROYECTO DE TRABAJO DE GRADO

ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA NORMA ISO27001:2013, EN ENTORNOS VIRTUALIZADOS SOBRE LA HERRAMIENTA HYPER-V LA EPS EN LIQUIDACIÓN.

DIANA MARCELA SALAMANCA ROJAS

JAIME ANDRES ROZO BOLIVAR

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

AÑO 2020

PROYECTO DE TRABAJO DE GRADO

ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA NORMA ISO27001:2013, EN ENTORNOS VIRTUALIZADOS SOBRE LA HERRAMIENTA HYPER-V LA EPS EN LIQUIDACIÓN.

DIANA MARCELA SALAMANCA ROJAS

JAIME ANDRES ROZO BOLIVAR

Trabajo de grado para optar al título de Especialista en Seguridad de la Información

Docente

DIEGO OSORIO
Docente Ing. de Sistemas y Computación
Facultad de Ingeniería
Universidad Católica de Colombia

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

AÑO 2020

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

1. INTRODUCCIÓN

La seguridad informática es el área perteneciente a la rama de la informática, que se enfoca en la infraestructura computacional permitiendo resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos, como lo hace referente la ISO/IEC 27001:2013 permitiendo así a las organizaciones mejorar la gestión de sus riesgos de seguridad de la información.
En la actualidad se debe ser conscientes de que en las empresas existen amenazas las cuales por no tener una parametrización y políticas de seguridad generan vulnerabilidades que pueden ser aprovechadas para comprometer los datos y la información de la empresa.

Las soluciones de virtualización de infraestructura mejoran la agilidad y flexibilidad de los servicios tecnológicos que a su vez permiten un ahorro de costo de equipos y procesos de mantenimiento.

Hyper-V, es una plataforma virtualizada que permite que varios sistemas operativos aislados compartan una misma plataforma de hardware., teniendo en cuenta lo anterior es la mejor herramienta a utilizar para crear y administrar las máquinas virtuales de la empresa, para darle el mejor manejo a la información en tiempo real, haciendo de este proyecto un recurso innovador para la empresa, esto teniendo en cuenta que se maneja información importante y sensible, la cual con esta tecnología vamos a lograr mitigar al máximo las amenazas y riesgos que se puedan presentar.

2. GENERALIDADES

2.1. LÍNEA DE INVESTIGACIÓN

La investigación que se realizó en este proyecto fortaleció la seguridad de la información de los servicios tecnológicos que se implementaron en la EPS en Liquidación, basados en la tecnología de virtualización en Hyper-V, aplicando herramientas y técnicas para validar la existencia de vulnerabilidades en sistema operativos, y los posibles ataques que se puedan presentar.

En la actualidad la incursión de las Tecnologías de la Información y Comunicaciones (TIC), a nivel global ha generado un impacto realmente significativo y esto nos ha dado como resultado la convergencia tecnológica, ya que la tecnología es un recurso fundamental para aquellas empresas que desean una herramienta con la que puedan lograr la optimización y mejorar los procesos aplicando las mejores prácticas del sector.

La empresa cuenta con la tecnología de virtualización Hyper-v, la cual permite crear entornos de servidores virtuales que permiten a su vez administrar múltiples sistemas operativos en un solo servidor físico, optimizando así de manera eficaz y segura el manejo de la información de la EPS en Liquidación, la cual se dedica al aseguramiento en salud de los ciudadanos con y sin capacidad de pago.

2.2. PLANTEAMIENTO DEL PROBLEMA

El problema a resolver en la empresa EPS EN LIQUIDACIÓN surge de la necesidad de tener la administración centralizada de las bases de datos transaccionales tanto de consulta, como de la aplicación, para lograr una reducción de costos y coadministrar la información de los diferentes usuarios que en su momento tenían servicios con la EPS y así obtener de manera oportuna, disponible e integra los datos requeridos, para dar respuestas más rápidas a los entes de control pertinentes.

Por eso se implementará una solución a nivel de una infraestructura en sitio donde se ofrecerá el esquema de la seguridad de la información de las diferentes bases de datos y aplicaciones que maneja la organización, a través de la aplicación de los controles y herramientas de gestión dados por la Norma ISO-27001:2013.

2.2.1. ANTECEDENTES DEL PROBLEMA

Determinación del problema

Históricamente en los sistemas tecnológicos, siempre las grandes empresas han utilizados múltiples servidores físicos, cada uno para un trabajo específico ya sea

como servidor de aplicación, servidor de presentación, servidor de bases de datos, servidor de correo, servidor de dominio, entre otros, haciendo de esto una variable para cada servidor en cuanto a necesidades de CPU, memoria y almacenamiento a la hora de comprar o realizar algún cambio en hardware.

Esto ha mejorado con la llegada de las tecnologías de virtualización la cuales permitían dividir un servidor físico para el uso de varios servidores virtualizados por individual lo que permitía asignar la CPU, memoria y almacenamiento del servidor físico para recursos de los servidores virtualizados y asignarlos para varias cargas de trabajo de manera simultánea.

La tecnología de virtualización permite equilibrar las cargas de una forma más inteligente y eficiente debido a que esta permite la reasignación de recursos en caliente, (ambientes productivos), sin necesidad de generar una indisponibilidad, ni detención de la operación.

No se debe confundir el término de virtualización con servicios en la nube ya que son dos términos totalmente diferentes. La computación en la nube hace referencia al intercambio de recursos informáticos entregados como servicio a través de internet y la virtualización hace referencia a la manipulación de un servidor físico pueda ser compartido para varias máquinas virtuales por múltiples sistemas operativos.

El cloud computing o servicios en la nube cobra cada vez más relevancia en las empresas debido, principalmente, a la ventaja de no tener que hacer grandes inversiones en infraestructuras que mantengan aplicaciones, plataformas o servidores propios. Infraestructura como Servicio - IaaS, Plataforma como Servicio -PaaS y Software como Servicio -SaaS, es el futuro, y cada vez están más en el presente de múltiples empresas.

El modelo más conocido es la Cloud pública, cuyos servidores se ofrecen dentro de un entorno virtualizado a través de una red pública como Internet, y los usuarios se benefician de una misma infraestructura compartida en la que definen a medida sus recursos y pagan sólo por lo que usan.
Dentro de los Servicios en la Nube se enmarcan tres conceptos fundamentales: IaaS, PaaS y SaaS.

Las tecnologías de virtualización o plataformas se reconocen con el nombre hipervisores. Hoy en día, existen varios hipervisores en el mercado tecnológico los más conocidos o usados son: Vmware ESXI y VSphere,KVM (Open Source Hypervisor y RHEV (Red Hat Enterprise Virtualization) y Hyper-V esta última siendo la versión de Microsoft y la seleccionada a utilizar para este proyecto.

¿Por qué virtualizar en Hyper V?

A diferencia de lo que ofrecen la mayoría de hipervisores los cuales, ofrecen características de crear y administrar máquinas virtuales, este también permite la

facilidad de que estas máquinas puedan permanecer separadas del resto de su sistema operativo, lo que las convierte en un entorno ideal para equilibrar cargas de trabajo.

Las máquinas virtuales son más fáciles de administrar que el hardware físico y no tienen un gasto tan alto, además que el licenciamiento no tiene un límite de utilización como si pasa por ejemplo en hipervisores de VMWARE, por ejemplo, Hyper-V permite crear máquinas virtuales según sea la capacidad que tenga el servidor físico.

Los servidores físicos ante una emergencia catastrófica como incendio o inundación, terremoto en un data center, pueden ocasionar daños de hardware, daños eléctricos, entre otros, esto no permitiría dar la continuidad de negocio tan rápida y en su totalidad de operación, por eso con la llegada de tecnologías de virtualización las máquinas virtuales que se creen, pueden reducir el tiempo de inactividad e indisponibilidad ante una catástrofe como las mencionadas, ya que las cargas de trabajo en ejecución se pueden copiar más ágilmente y de manera fácil y se puede trasladar el servidor afectado a otro servidor sin interrupciones, ya que Hyper-V permite configurar una réplica de estos máquinas en otro lado o migrarlas de manera muy rápida. También se pueden configurar para reiniciar automáticamente las Virtual Machine -VM, afectadas por fallas del servidor.

Por lo anterior y teniendo en cuenta que el término de seguridad informática se relaciona con el conjunto de herramientas, controles y buenas prácticas expresadas en la norma 27001:2013. informáticas que permiten la protección a la información y a los equipos que los contienen teniendo como objetivo la confidencialidad disponibilidad e integridad de estos.

En la actualidad las organizaciones son cada vez más dependientes de alguna manera de la tecnología de la información como una herramienta esencial para lograr sus objetivos de negocio o para poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy.

Los riesgos de la información están presentes cuando intervienen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones.

2.2.2. PREGUNTA DE INVESTIGACIÓN

¿Cómo un esquema de seguridad de la información, basado en la norma ISO27001:2013, permitirá fortalecer la seguridad de la información en tecnologías de virtualización como Hyper-V?

2.3. JUSTIFICACIÓN

Las infraestructuras basadas en máquinas virtuales tienen cada día más presencia, debido al ahorro de costos y a las posibilidades de desplegar entornos ágiles, flexibles y dinámicos que puedan adaptarse a las necesidades del modelo de negocio en cada momento.

La seguridad de los equipos virtualizados y los sistemas informáticos que los sustentan debe ser una prioridad para asegurar los datos y servicios. En Windows Server el rol de Hyper-V proporciona varias herramientas para mejorar la seguridad de estas tecnologías.

Conocer los servicios y características de Hyper-V y las Máquinas Virtuales de Microsoft permite desplegar entornos basados en virtualización y utilizar las capacidades virtuales para mejorar la seguridad a nivel de red, en los servicios perimetrales y en las máquinas virtuales y en la ejecución segura de aplicaciones o la gestión de credenciales.

Al analizar la problemática de la EPS en LIQUIDACION por su misma palabra "liquidación" se ve expuesta a problemas económicos y la idea es minimizar sus gastos, pues la empresa pagaba un arrendamiento por sus servicios de bases de datos, donde se llega a la conclusión de que al pagar alquiler de los servidores dedicados a lo largo de los años la suma excede el precio y la información nunca es solamente de la empresa, sino del proveedor que dispone los servicios tecnológicos, por esto se busca una solución pues la idea era reducir costos y proteger la información.
La implementación de entornos virtuales añade puntos de riesgo en su forma de despliegue debido a que, en ocasiones no se consigue el 100% de sinergia entre el software de virtualización y el hardware de alojamiento. Los criminales informáticos se enfocan principalmente en explotar las vulnerabilidades de los sistemas, sean físicos o virtuales y desarrollan malware avanzado con ataques altamente orientados para aprovechar estos fallos y/o brechas. Si un atacante consigue filtrase al sistema virtual, puede escapar al equipo anfitrión y comprometer las demás máquinas, así como los equipos. Las soluciones de seguridad convencionales no cubren los requerimientos de cumplimiento y protección para hipervisores y máquinas virtuales, ya que no ofrecen mecanismos de seguridad que involucren plenamente las condiciones propias para ambientes virtuales, tendencias como la nube o centros de datos definidos por software (SDDC).

Por las razones antes expuestas se llegó a la conclusión de que era necesario implementar un sistema de virtualización basado en tecnología de hypervisor, la finalidad de hacer la instalación en Hiperv, es la de tener un control de mecanismos de seguridad y autogestionar con la administración su correcto funcionamiento, que permitan a su vez mejorar la continuidad del negocio. A partir de instalación buscamos plantear un esquema de seguridad de la información, basado en la norma ISO27001:2013, la cual garantiza la preservación de la confidencialidad, integridad y disponibilidad de la información, al igual que la protección de los datos en entornos

virtualizados sobre la herramienta Hyper-v para la EPS EN LIQUIDACIÓN.

Todo esto permitirá facilitar el acceso a una nube privada en donde se almacenará la información dando a esta, una seguridad, ya que hoy en día es fundamental por las amenazas y vulnerabilidades que se presentan, la idea es tomar ventajas de la herramienta que nos de una forma segura y eficaz para aprovechar al máximo el rendimiento de esta, optimizando recursos y teniendo herramientas propias de la empresa dándole seguridad a los datos ya que se manifiesta que son personales y delicados que no pueden ser susceptibles o abiertos para otras personas.

2.4. OBJETIVOS

2.4.1. OBJETIVO GENERAL

Plantear un esquema de seguridad de la información, basado en la norma ISO27001:2013, en entornos virtualizados sobre la herramienta Hyper-V de la EPS EN LIQUIDACIÓN.

2.4.2. OBJETIVO ESPECÍFICOS

- Identificar los riesgos y estándares de seguridad para la virtualización de los servidores con tecnología Hyper-v en un entorno Cloud.
- Evaluar las vulnerabilidades en los servidores virtuales de la EPS EN LIQUIDACIÓN.
- Estructurar el esquema de seguridad a partir de la identificación de los riesgos y amenazas, realizar evaluación de vulnerabilidades y estándares de seguridad para los entornos virtualizados sobre la herramienta Hyper-v de la EPS EN LIQUIDACIÓN.

2.5. CRONOGRAMA

CRONOGRAMA DEL PROYECTO										
Actividad del Proyecto*	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE
1. ANTEPROYECTO										
Seleccionar Tema										
2. DESARROLLO										
Titulo										
Linea de Investigación										
Planteamiento del Problema										
Justificacion										
Objetivos										
Cronograma y Presupuesto										
Marcos de Referencia										
Estado del arte										
3. METODOLOGIA										
Enfoque y estudio de investigación										
Recoleccion de datos y aplicación de herramientas										
Analisis de información										
Revision de riesgos y estándares de seguridad para la virtualización de los servidores										
Evaluación las vulnerabilidades en los servidores virtuales										
Estructuración esquema de seguridad										
4. RESULTADOS										
Resultados de la aplicación de la metodologia										
Esquema de seguridad										
5. CONCLUSIONES Y RECOMENDACIONES										
Conclusiones y recomendaciones										
Entrega de trabajo y entregables										
Sustentacion de proyecto de especialización										

Figura 1 - 2 Cronograma

3. MARCOS DE REFERENCIA

La virtualización de los sistemas y herramientas se ha convertido en una de las soluciones más económica, provechosa y eficiente para dar respuesta a los problemas que se relacionan con el mejor aprovechamiento de estos recursos en la medida que les permite a las organizaciones darle un mejor uso y manejo de los recursos computacionales al mismo tiempo que logran disminuir el costo total asociado a los mismos.

La virtualización ha tenido evidente aceptación en el mundo de TI en los últimos años, sin embargo, las amenazas no discriminan el tipo de ambiente y los daños son indistintamente perjudiciales para las organizaciones. Por tal motivo, la protección de última generación para el entorno virtual es imprescindible en el negocio a fin de mantener servicios confiables y disponibles.

3.1. MARCO CONCEPTUAL

La seguridad informática sirve para garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas y de la información contenida en ellos, así como de las redes privadas y sus recursos. La seguridad informática debe vigilar la privacidad, la integridad, y la disponibilidad.

La virtualización de servidores es una tecnología basada en un software que posibilita la ejecución de varios sistemas operativos diferentes entre sí, como invitados dentro de un único host del servidor físico. Son las llamadas máquinas virtuales (VMs) que ejecutan en una imitación virtual del hardware del servidor. Es como si los recursos de un servidor físico, por ejemplo, fuesen divididos en diversos servidores virtuales que pueden ser usados con diferentes finalidades.

En la tecnología de Hyper v la distribución de almacenamiento se puede realizar por ISCSI, SAN en diferentes tipos de arreglos ya sea en RAID 1 A RAID 5.

Los arreglos más utilizados en las compañías son: en RAID 5 el cual ha logrado popularidad gracias a su bajo coste de redundancia. Generalmente, el RAID 5 se implementa con soporte hardware para el cálculo de la paridad. RAID 5 necesitará un mínimo de 3 discos para ser implementado.

3.2. MARCO TEÓRICO

La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

Existen también diferentes definiciones del término Seguridad Informática. De ellas nos quedamos con la definición ofrecida por el estándar para la seguridad de la información ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por

la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC).

“La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.”

A la hora de implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001, debemos considerar como eje central de este sistema la Evaluación de Riesgos. Este capítulo de la Norma, permitirá a la dirección de la empresa tener la visión necesaria para definir el alcance y ámbito de aplicación de la norma, así como las políticas y medidas a implantar, integrando este sistema en la metodología de mejora continua, común para todas las normas ISO.

Lo primero, es elegir una metodología de evaluación del riesgo apropiada para los requerimientos del negocio. Existen numerosas metodologías estandarizadas de evaluación de riesgos. Aquí explicaremos la metodología sugerida en la Norma.

Las fases de esta metodología son los siguientes:

Figura 1 - 3 Fases esquema ISO 27001

Reconocer los Activos de Información y sus responsables, comprendiendo por activo todo aquello que tiene valor para la empresa, incluyendo soportes físicos (edificios o equipamientos), intelectuales o informativas (Ideas, aplicaciones, proyectos ...) así como la marca, la reputación etc.

Reconocer las Vulnerabilidades de cada activo: aquellas debilidades propias del activo que lo hacen susceptible de sufrir ataques o daños.

Reconocer las amenazas: Aquellas cosas que puedan suceder y dañar el activo de la información, como ataques de virus, incendios o, desastres naturales espionaje etc.

Reconocer los requisitos legales y contractuales que la empresa está obligada a cumplir con sus clientes, socios o proveedores.

Reconocer los riesgos: Definir para cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información, en relación a su disponibilidad, confidencialidad e integridad del mismo.

Cálculo del riesgo: evalúan la probabilidad y las consecuencias de que ocurra un incidente en particular. El proceso consiste en la evaluación de la vulnerabilidad de un proyecto en un riesgo determinado.

Plan de tratamiento del riesgo: se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad. En este punto, es donde seleccionaremos los controles adecuados para cada riesgo, los cuales irán orientados a :

- ✓ Asumir el riesgo
- ✓ Reducir el riesgo
- ✓ Eliminar el riesgo
- ✓ Transferir el riesgo

¿Qué es la virtualización?

La virtualización es una tecnología que permite crear servicios de TI útiles mediante recursos que están ligados tradicionalmente al hardware. Además, distribuye sus funcionalidades entre diversos usuarios o entornos, lo que permite utilizar toda la capacidad de una máquina física. como, por ejemplo, aplicaciones, servidores, redes y almacenamiento virtuales. Es la forma más eficaz de reducir los gastos de TI y, a la vez, aumentar la eficiencia y la agilidad para empresas de cualquier tamaño.

¿Cuáles son los riesgos de seguridad con la virtualización?
La virtualización tiene que administrarse adecuadamente para mantener los datos de la empresa seguros. Debido a que las máquinas virtuales son copias de sus servidores, cuantas más máquinas virtuales tenga, más objetivos debe proteger de los atacantes que deseen acceder a sus datos confidenciales. Esta vulnerabilidad

de seguridad hace que sea importante contar con una solución de administración centralizada para supervisar las máquinas virtuales y protegerlas de un acceso no autorizado. La seguridad de la virtualización es un elemento esencial de la infraestructura de escritorios virtuales o VDI

Microsoft, Hyper-V y máquinas virtuales

Básicamente, una máquina virtual es un programa de ordenador que utiliza el hardware real para comportarse como un PC (CPU, RAM, tarjeta gráfica, disco duro, periféricos…).

El camino de Microsoft por crear una herramienta de virtualización profesional no termina con Virtual PC. En 2008 lanzó Hyper-V, una tecnología que, mediante software y aprovechando los procesadores de 64-bits, permite virtualizar un segundo o tercer sistema operativo, siempre y cuando el hardware lo permita.

Las ventajas de Hyper-V son, principalmente, que se encuentra integrado con Windows, por lo que se aprovechan mejor los recursos de software y hardware y se evitan incompatibilidades.

Principales ventajas de Microsoft Hyper-V para tu negocio

A continuación, vamos a concretar cuáles son las ventajas de la virtualización y, más en concreto, la virtualización a través de Hyper-V.

- Ahorro en costes de hardware.
- Visualización nativa de 64 bits.
- Optimización de la gestión de la información de la empresa.
- Recuperación de estados anteriores a través de instantáneas.
- Reducción de los tiempos de implementación.
- Capacidad de ejecutar máquinas virtuales de 32 y 64 bits de uno o varios procesadores.
- Facilitación del backups de los datos de la empresa.
- Capacidad de realizar migraciones en vivo.
- Apoyo para alcanzar determinadas metas empresariales.
- Mejora de la continuidad empresarial.
- Establece o amplia un entorno de nube privado.

La parte de **administración** de este sistema es muy relevante porque nos aporta unas ratios de máquinas virtuales superior al de otros fabricantes. Igualmente, analiza el tráfico IP de una determinada dirección o máquina virtual para asegurar en todo momento que la carga de trabajo sea la correcta.

3.3. MARCO JURÍDICO

Decreto No. 1360 de 1989 Reglamenta la inscripción del soporte lógico (software)en el Registro Nacional del Derecho de Autor. El soporte lógico (software) será catalogado como obra inédita siempre y cuando no lo haga manifiesto el titular de los derechos de autor. La protección del derecho de autor al soporte lógico no excluye otras formas de protección por el derecho común.

La Ley 1273 de 2009 Ley de Delitos Informáticos en Colombia

Declara, preserva y protege los derechos que tenemos las personas de acceder a un sistema informático seguro, ya que impone sanciones que van desde 48 a 96 meses de prisión, hasta multas de 100 a 1500 salarios mínimos legales vigentes, además de la pena de inhabilitación para el ejercicio de profesión relacionada con sistema de información procesada con equipos computacionales, por los siguientes delitos.

1. Acceso abusivo a un sistema informativo
2. Obstaculización ilegitima de sistema informativo o red de telecomunicación
3. Interceptación de datos informáticos
4. Daño informático
5. Uso de software malicioso (virus)
6. Violación de datos personales
7. Suplantación de sitios Web para capturar datos personales
8. Circunstancia de agravación punitiva
9. De los atentados informáticos y otras infracciones

Ley 1581 de 2014 Protección de datos personales.

La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Las empresas deben aprovechar la expedición de estas leyes o decretos para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información.

Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo desde casa, este es un ejemplo de nuestra actualidad pues la mayoría de gente nos encontramos en estos momentos trabajando de esta

manera lo que exige un nivel más alto de supervisión ya que la gente manipula la información desde un lugar distinto o un pc diferente.

Resulta adecuado dictar charlas y seminarios al interior de las organizaciones con el fin de que los trabajadores sean conscientes de las leyes que se ejercen en la actualidad por estos delitos informáticos, pues también es necesario que el empleado este enterado a que se puede exponer al tratar de realizar un fraude y a que lo pueden con llevar el uso inadecuado de la información de la empresa.

Con la promulgación de estas leyes se obtiene un mecanismo importante para denunciar los hechos delictivos a los que se pueda ver afectada la empresa, pues las empresas muchas veces deciden no denunciar o el desconocimiento de las leyes hacen como si no pasara nada por eso siempre la seguridad en una compañía no será un gasto si no una inversión ya que en las empresas existe información de diferente tipo o clase pero que siempre será importante. La información es un recurso vital para toda organización, y el buen uso de ésta puede significar la diferencia entre el éxito o el fracaso para una empresa.

3.4. ESTADO DEL ARTE

24 Estadísticas de Seguridad Informática que Importan en el 2019

Los ciberataques y las brechas de seguridad se están volviendo un hecho diario, por lo que es más importante que nunca proteger tanto a los computadores de tu negocio, como a los propios.

Seguridad Informática

El 70% de las organizaciones cree que su riesgo de seguridad creció considerablemente en el 2017. Se estima que para el 2020, el número de contraseñas utilizadas crecerá a 300 billones. 43% de los ciberataques afectan a pequeños negocios. A una compañía le toma entre 6 meses, o 197 días, detectar una brecha de seguridad.

Costos de la Seguridad Informática

El mercado de la seguridad informática crecerá un 8.7% en el 2019, llegando a los $124 billones. El costo total de un ciberataque exitoso es de más de $5 millones de dólares, o $301 por empleado. La brecha de seguridad de Equifax le costó más de $4 billones a la empresa. Las empresas gastan un estimado de $2.4 millones en defensa.

Entender el estado actual de la seguridad informática es importante para poder proteger tus equipos, tu familia y tus negocios de las amenazas digitales. Entonces… ¿Qué puedes hacer para proteger tus equipos? El primer paso es estar educado y mantenerse actualizado acerca de las últimas amenazas.

Una gran ventaja de ahorrar presupuesto es virtualizar con Hyper v por su forma de licenciamiento.

Microsoft ofrece una licencia de Windows Server DataCenter de forma gratuita a todos los clientes que migren su infraestructura de VMware a Hyper-V

Ahora, el gigante de Seattle ofrece de forma gratuita una licencia de Windows Server DataCenter, el servidor virtual de la compañía, a aquellos clientes que migren su infraestructura digital de VMware a Hyper-V. La oferta, que ya ha entrado en vigor, está dirigida a aquellos clientes que estén pensando en disminuir costes en infraestructura VMware, ya sea por finalización del contrato existente u otras razones, migrando a entornos basados en Hyper-V. El plan pone foco en clientes que ven el factor económico como un gran obstáculo y también en aquellas Empresas que estén pensando en desplegar hosts de Hyper-V en su infraestructura porque consideran la visión de nube de Microsoft una ventaja. Según Microsoft, los beneficios para los clientes de migrar de VMware a Hyper-V son varios.

También Hyper-V permite la gestión centralizada de la seguridad. Con el paso del tiempo, la plataforma Hyper-V de Microsoft es cada vez aceptada con mayor confianza por los profesionales de IT. Atrás ha quedado el irregular desempeño de Hyper-V en 2008. Hyper-V ha ganado terreno rápidamente y ha demostrado que puede alcanzar los mismos y mejores niveles en eficiencia, seguridad, escalabilidad y costos, que los principales referentes en virtualización.

Microsoft ha anunciado la funcionalidad de "Hyper-V Recovery Manager" en Windows Azure, lo cual permite elaborar una estrategia de Disaster Recovery Plan a través de una consola integrada en la nube entre dos sitios on-promises. Microsoft ha adicionado en Hyper-V la posibilidad de administrar los recursos cuando se estén realizando operaciones de migración en caliente, por lo cual se dará prioridad a otras tareas cuando se programa una migración. Hyper-V en Windows Server 2012 R2 permite realizar la clonación y la exportación en caliente de máquinas virtuales sin la necesidad de apagarlo como en versiones anteriores.

4. METODOLOGÍA

4.1. FASES DEL TRABAJO DE GRADO

Para realizar la siguiente investigación la cual abarca el tema principal de plantear un esquema de seguridad de la información bajo la norma ISO27001 2013 para las diferentes aplicaciones en entornos virtuales con los requisitos basados en el ciclo PHVA para cumplir con las buenas prácticas en la empresa EPS en liquidación.

Se realizará una validación de los riesgos, vulnerabilidades, amenazas y estándares de seguridad en virtualización en Hyper-V con diferentes herramientas de escaneo e identificación de vulnerabilidades en los sistemas operativos para poder identificarlas y proceder a dar un diagnostico o informe ejecutivo de cuáles son las mejores acciones y buenas prácticas para realizar una virtualización en un entorno cloud y definir que esquema de seguridad se debe implementar para minimizar posibles ataques y mantener en lo posible la integridad, disponibilidad y confidencialidad de los datos e información, cabe aclarar que en seguridad de la información no se garantiza el 100 % .de la protección de los datos pero si minimizar el umbral de amenazas o ataques.

Para todo esto se procederá a llevar a cabo estas validaciones de vulnerabilidades y riesgos, la creación de una maquina con unas características de hardware especificas con Kali Linux, se procederá a instalar NESUS y a involucrar esa máquina en la red de datos de la empresa en el segmento donde se encuentran los servidores virtualizados para realizar un escaneo y observar la vulnerabilidades más críticas, luego validar si es posible corregirlas ya sea con un parche de actualización, configuración o parametrización del sistema operativo o algún dispositivo.

4.2. INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Las herramientas a utilizar serán el sistema operativos de linux con las aplicaciones de NESSU ,NMAP Y METASPLOIT la cuales realizan las siguientes acciones:

Nessus: es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron.

Nmap: Este software posee varias funciones para sondear redes de computadores, incluyendo detección de equipos, servicios y sistemas operativos. Estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Además, durante un escaneo, es capaz de adaptarse a las condiciones de la red incluyendo latencia y congestión de la misma.

Metasploit: Su subproyecto más conocido es el Metasploit Framework, una herramienta para desarrollar y ejecutar exploits contra una máquina remota. Otros subproyectos importantes son las bases de datos de opcodes (códigos de operación), un archivo de shellcodes, e investigación sobre seguridad.

Software base Kali Linux, Nmap, Metasploit.: Este software ya viene en un export y configurada la maquina con toda su respectiva configuración y seguridad para ejecutarla en producción y realizar un escaneo de vulnerabilidades dentro la red del cliente.

4.3. ALCANCES Y LIMITACIONES

Con este proyecto se pretende realizar un escaneo a una infraestructura de seguridad a unos servidores virtualizados en Hyper-V, desde el host principal como las máquinas virtuales, el 100 % de la seguridad no se puede garantizar, pero si bajar el umbral de vulnerabilidades y mitigar las amenazas hacia la infraestructura. Limitantes serias no tener acceso a la red o los servidores a validar las vulnerabilidades.

5. PRODUCTOS A ENTREGAR

Informe detallado de las vulnerabilidades encontradas en la infraestructura del cliente: Evaluar las vulnerabilidades encontradas y realizar un informe ejecutivo con los hallazgos o huecos de seguridad encontrados, informar al cliente que buenas prácticas debe tener en cuenta en su infraestructura.

Informe ejecutivo y explicación de parchado en servidores infraestructura cliente.: Una vez se realice el escaneo de vulnerabilidades en los servidores se procederá a mirar el parchado de los servidores y se indicara en un informe cual es la mejor practica de hacer esta actividad, recomendaciones por Microsoft.

Pruebas de Pentesting: una vez se realice las recomendaciones de seguridad dadas en el informe se procederá a realizar un escaneo y pruebas de Pentesting validando que los huecos e seguridad encontrados ya fueron mitigados.

Análisis de Brecha ISO27001. El análisis de brecha ISO 27001 con la herramienta web de 27001 Academia, al cual se puede acceder desde el url http://advisera.com/27001academy/es/herramientas/herramienta-gratuita-analisis-debrecha-para-iso-27001/.

Y las recomendaciones de uso de la aplicación y su mantenimiento para una buena ejecución.

6. RESULTADOS ESPERADOS E IMPACTOS

El proyecto dará como resultado que la EPS en liquidación tenga un esquema de seguridad en su infraestructura implementada para que la información migrada del datacenter externo tenga los tres pilares de la seguridad de la información integridad, confidencialidad y disponibilidad para minimizar las vulnerabilidades en la red, servidores y aplicaciones de la empresa bajo la norma ISO27001:2013.

7. ENTREGA DE RESULTADOS E IMPACTOS

Debido a la importancia que tiene la información de la EPS en Liquidación, se optó por utilizar la norma ISO 27001:2013, ya que permitirá de alguna manera ponerles valor a los riesgos, proteger la confidencialidad, integridad y disponibilidad de la información. Esto se hace identificando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

ALCANCE
para cumplir el objetivo propuesto, el desarrollo del trabajo cubrió:

Las oportunidades de mejora registradas para los procesos presentados a continuación:

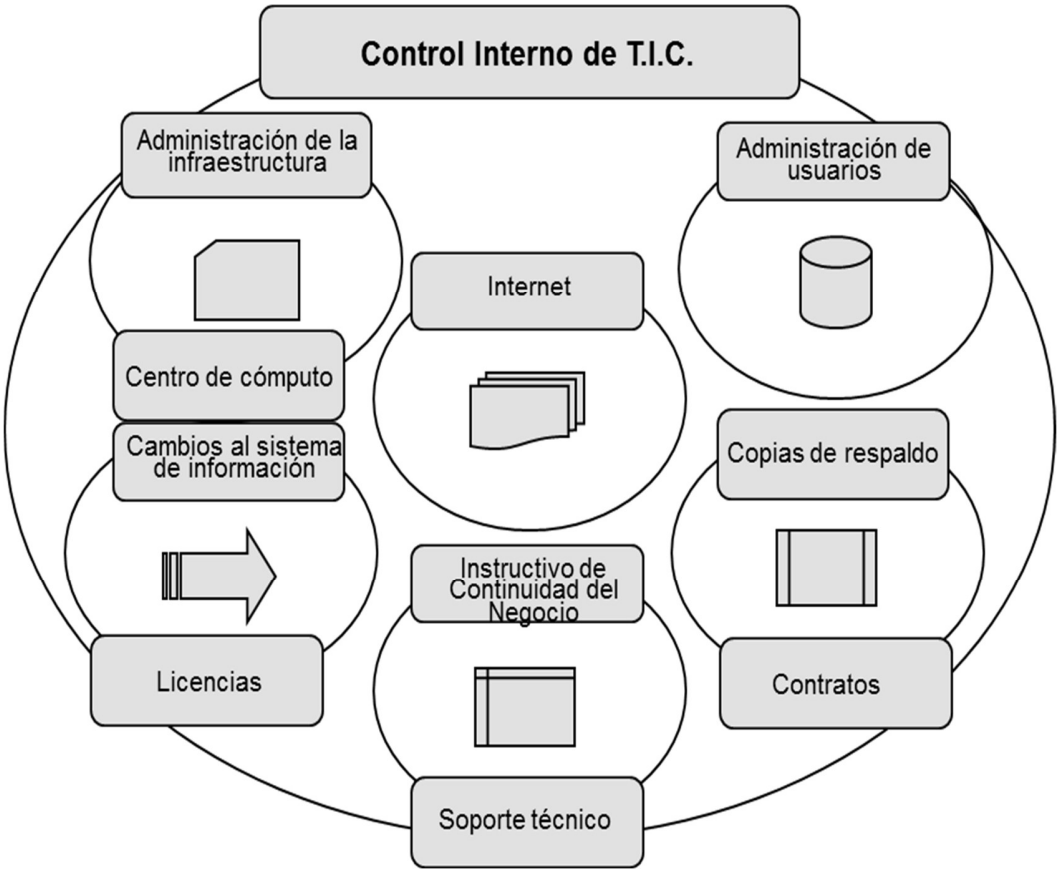


Figura 1 - 4 Infraestructura control empresa

Metodología.
Se llevaron a cabo entrevistas con el funcionario.

Obtención y análisis de evidencias documentales aportadas por la administración.

LEVANTAMIENTO DE INFORMACION PARA LA EVALUACION DEL PROCESO DE LA EPS SA EN LIQUIDACION			
DESCRIPCION DE LA ACTIVIDAD	**RESPONSABLE**	**TIPO DE ENTREGA**	
		FISICO	**MEDIO MAGNETICO**
INFORMACIÓN REQUERIDA			
Organigrama del área de TIC	ALEJANDRO		
Diagrama de infraestructura tecnológica y de comunicaciones	ALEJANDRO		
Diagrama de sistemas de información	ALEJANDRO - JAIME		
Matriz de sistemas de información, donde se indique:	ALEJANDRO - JAIME		
Nombre de la aplicación, sistema de información o ERP			
Número de usuarios			
Directos (aquellos que pueden ingresar, modificar, borrar información)			
Indirectos (aquellos que consultan información)			
Interfaces (con que aplicaciones tiene, bien que genera o recibe)			
Descripción de las modificaciones o mantenimientos a la aplicación en el año 2020			
Herramienta en la cual está desarrollada			
Es desarrollo interno o adquirido (en caso de ser adquirido, quien es el proveedor)			
ORGANIZACIÓN Y ADMINISTRACIÓN			
Documentación asociada a la parametrización Firewall, antivirus.	CAMILO		
Documentación asociada al centro de cómputo o centro de comunicaciones.	ALEJANDRO		
Inventario de licencias de software	JAIME		
ADMINISTRACION DE USUARIOS (ASIGNACIÓN DE ROLES Y PERFILES)			
Documentación o procedimientos para administración de usuarios (componentes tecnológicos y de usuarios funcionales de aplicaciones o sistemas de información)	CAMILO - CRISTIAN		
Matriz de roles y perfiles para la asignación de los permisos en los sistemas de información	CAMILO - CRISTIAN		
INTERNET/INTRANET/EXTRANET			
Políticas del uso de Internet/Intranet, correo electrónico	CAMILO - CRISTIAN		
Perfiles en el directorio activo	CAMILO - CRISTIAN		
Bloqueos de acceso a Internet	CAMILO - CRISTIAN		
COPIAS DE RESPALDO			
Que tipos de copias de respaldo. Diario. Interno. Externo	JAIME - CRISTIAN		
Captura de la tarea programada	JAIME - CRISTIAN		
evidencias de copias de respaldo	JAIME - CRISTIAN		

Almacenamiento externo	JAIME - CRISTIAN		
SOPORTE TÉCNICO			
¿Cómo se gestionan los incidentes TIC?	CAMILO - CRISTIAN		
Procedimientos para dar soporte a la infraestructura tecnológica (servidores, impresoras, equipos de escritorios, portátiles, dispositivos móviles, etc)	CAMILO - CRISTIAN		
CAMBIOS A LOS SISTEMAS DE INFORMACIÓN			
¿Cómo se gestionan las solicitudes de cambio al sistema de información?	CAMILO - CRISTIAN		
Procedimiento para cambios o modificaciones a las aplicaciones, los sistemas de información y/o ERP	CAMILO - CRISTIAN		
PLAN O INSTRUCTIVO DE CONTINGENCIA			
¿Existen un plan o instructivo de contingencias?	ALEJANDRO		
¿Existen planes asociados a la continuidad del negocio?	ALEJANDRO - CAMILO		
Matriz de riesgo tecnológico	ALEJANDRO		
ADMINISTRACION DEL CENTRO DE CÓMPUTO O DE COMUNICACIONES			
Plano de la ubicación y distribución de los componentes tecnológicos en el centro de cómputo.	ALEJANDRO		
Planos de sistema eléctrico y cableado estructurado	ALEJANDRO		
Descripción de los mecanismos de seguridad.	ALEJANDRO		
LICENCIAS DE SOFTWARE			
Inventario de los equipos de cómputo y de las licencias de software asignadas.	JAIME		
CONTRATOS			
Relación de los contratos que tiene con terceros para prestación de servicios, soporte o mantenimientos con relación a la infraestructura tecnológica, etc.	ALEJANDRO		
ASPECTOS CLAVES LEY 1581 DE 2012			
1. Inscripción de las bases de datos en la SIC	JAIME		
2. Política de tratamiento de la información personal			
3. Divulgación de la política de protección de datos (publico)			
4. Aviso de privacidad y formato de autorización del titular (clientes, proveedores, contratistas y empleados)			
5. Herramientas que garanticen condiciones de seguridad adecuadas para evitar la adulteración, pérdida, consulta, uso o acceso fraudulento sobre la información. Medidas tecnológicas para proteger los datos personales y sensibles.			

6. Manual interno de políticas y procedimientos para cumplir con la Ley sobre protección de datos.			
7. Procedimientos operacionales para obtener la autorización del titular previo al inicio del tratamiento.			
8. Gestión de solicitudes del titular de la información. Conducto regular y canales físicos y electrónicos definidos para que el titular ejerza sus derechos de acceso, rectificación y supresión. (eliminar, actualizar, quejas, revocar autorización).			
9. Comité Habeas Data. Definir o crear un área o sujeto responsable de la protección de la información personal, según el tamaño empresarial del cliente (es decir aquí opera el criterio de responsabilidad demostrada consagrado en el art. 23 del Decreto 1377).			
10. Divulgación, formación y educación			
11. Sistema de administración de riesgos asociados al tratamiento de datos personales.			

Tabla 1 - 1 Tabla para el levantamiento de información.

Esta información requerida es con la que levantamos las bases para revisar los riesgos y las vulnerabilidades, no está plasmada por permisos de la Eps en Liquidación, pero sobre la recolección de datos armamos nuestras matrices, recomendaciones y conclusiones.

7.1. EVALUACIÓN DE VULNERABILIDADES

Esta evaluación muestra las vulnerabilidades en las aplicaciones que se utilizan en la operación diaria para la Eps en Liquidación y los servidores donde están instaladas las aplicaciones, este análisis se realizó enfocado a los servidores web y los servicios que están físicos donde se contienen las máquinas virtuales, adicional a la información que esta almacenada en estos.

En esta primera parte podemos ver la identificación de los servidores la evidencia de los activos físicos y una muestra de algunos servidores para saber que las tomas de información son reales.

ACTIVOS INFRAESTRUCTURA SERVIDORES EPS EN LIQUIDACION

Nombre Del Servidor	Aplicacion	Tipo de Ambiente	Capa	Cores Virtuales	Velocidad	RAM - Ficha GB	Particionamiento	IP Local	SO	SERVIDOR
CFBGTCYWDC01	ACTIVE DIRECTORY	PRODUCCION	AD	6	2,7	32	C:256GB	10.127.96.2	Microsoft Windows Server 2012 R2 Standard	VIRTUAL
CFBGTCYWDWH01	BD_CAFESALUD	PRODUCCION	BASE DE DATOS	12	3,5	160	C: 512 E: 3,584 F: 2,048 G: 1,000 H: 512 I: 3,9	10.127.96.4	Microsoft Windows Server 2012 R2 Standard	VIRTUAL
CFBGTCYWINFODB0	BD Infopoint tutelas	PRODUCCION	BASE DE DATOS	12	3,2	12	C: 500 E: 2,572	10.127.96.5	Microsoft Windows Server 2012 R2 Standard	VIRTUAL
CFBGTCYWINFOAPP	APLICACIÓN INFOPOINT TUTELAS	PRODUCCION	APLICACIÓN	6	3,2	8	C: 200E: 312	10.127.96.6	Microsoft Windows Server 2012 R2 Standard	VIRTUAL
CFBGTCYWDBS01	BD Operaciones y afiliaciones	PRODUCCION	BASE DE DATOS	8	3,2	32	C: 100 E:3,100	10.127.96.10	Microsoft Windows Server 2012 R2 Standard	VIRTUAL
CFBGTCYWFIL01	FTP	PRODUCCION	FTP	6	3,2	16	C: 100 E: 2,200 F: 40 G: 140 H:350	10.127.96.11	Microsoft Windows Server 2012 R2 Standard	VIRTUAL
CFBGTCYWATDBBK02	Aletheia	PRODUCCION	BASE DE DATOS	Intel Xeon Gold 6150	2,7	4	D LOG: 15 E DB: 100	10.127.96.14	Micrsoft Windows 2000 Service Pack 4	VIRTUAL
CFBGTCYWPRWEB01	Paginaweb	PRODUCCION	APLICACIÓN	4	3,2	16	/dev/mapper/os-root 60G 54G 5.8G 91% / devtmpfs 7.8G 0 7.8G 0% /dev tmpfs 7.8G 0 7.8G 0% /dev/shm tmpfs 7.8G 793M 7.0G 10% /run tmpfs 7.8G 0 7.8G 0% /sys/fs/cgroup /dev/sda1 509M 245M 265M 49% /boot /dev/mapper/os-home 864G 177G 688G 21% /home tmpfs 1.6G 0 1.6G 0% /run/user/0	10.127.96.15	CentOS Linux release 7.3.1611 (Core)	VIRTUAL
SEVENCFHN02	Seven	PRODUCCION	APLICACIÓN	4	2,4	8	C:51 GB D:20	10.99.1.17	MicrosoftWindows 2008 R2 Enterprise	VIRTUAL
SEVENCFHN01	Seven-Kactus	PRODUCCION	APLICACIÓN	4	2,4	8	C:46 D:409	10.99.1.82	MicrosoftWindows 2008 R2 Enterprise	VIRTUAL
CRYSTALSEVEN	Seven Reportes	PRODUCCION	APLICACIÓN	16	2,4	16	C:SYSTEM30GB D:DATOS20GB	10.99.1.129	Microsoft Windows Server 2003 Enterprise	VIRTUAL
ADMINISTRAR	Seven-Kactus	PRODUCCION	BASE DE DATOS	20	2,4	60	Kactus: 24 GB	10.99.1.106	MicrosoftWindows 2008 R2 Enterprise	VIRTUAL
CRUXBLANCA	Infopointpqrs	PRODUCCION	BASE DE DATOS	20	2,4	60	Base de datos:134368.45MB	19.99.1.115	MicrosoftWindows 2008 R2 Enterprise	VIRTUAL
HEONINFOPATH	Infopointpqrs	PRODUCCION	APLICACIÓN							VIRTUAL
CAFESALUD	Cuentas Medicas - Habilitar -Prestar	PRODUCCION	BASE DE DATOS	20	2,4	70	Base de datos cuentas medicas HEON :6850756.33MB /HEON:159972.25 MB	10.99.1.114	MicrosoftWindows 2008 R2 Enterprise	VIRTUAL
SVRTICSCFMV	HOST FISICO	PRODUCCION	Host	8	3,4	32	E:DATA932	10.26.9.224	Microsoft Windows Server 2012 R2 Data Center	FISICO
SVRCRPDCF	Correspondencia	PRODUCCION	APLICACIÓN	6	3,4	8	C:SYSTEM 120 D:DATA 200	10.26.9.159	Microsoft Windows Server 2012 Standard	VIRTUAL
SVRCRPDBDCF	Correspondencia	PRODUCCION	BASE DE DATOS	8	3,4	16	C:SYSTEM 120 E:70 DATA F:400 DATA G:200 DATA	10.26.9.158	Microsoft Windows Server 2012 R2 Data Center	VIRTUAL
SVRTICSCF	HOST FISICO	PRODUCCION	Host	4	3,4	32	C:SYSTEM149 E:DATA932 F: DATA782	10.26.9.223	Microsoft Windows Server 2012 R2 Data Center	VIRTUAL
DACAFESALUDA	INTRANET	PRODUCCION	APLICACIÓN	6	3,4	8		10.26.9.215	Microsoft Windows 10 Pro	VIRTUAL
SVRCF	JURIDICA-FINANCIERA-MATRIZ	PRODUCCION	APLICACIÓN	6	3,4	4	C:SYSTEM 120 E:DATA 200	10.26.9.226	Microsoft Windows Server 2012 Standard	VIRTUAL
CFPRODUCCION	FINANCIERA	PRODUCCION	APLICACIÓN	4	3,4	6	D:DATA 15GB	10.26.9.216	Microsoft Windows 10 Pro	VIRTUAL

Figura 1 - 5 Inventario de activos infraestructura servidores

Esta es la evidencia del Centro de Proceso de Datos donde se concentran los recursos necesarios para el procesamiento de la información de la EPS en liquidación, acá encontramos físicamente los servidores anteriormente nombrados en el inventario.

Figura 1 - 6 Evidencia activos físicos

En estos pantallazos vemos la evidencia física de algunos de los servidores revisamos nombres de que están compuestos, cuales aplicaciones y que sistema operativo manejan.

CFBGTCYWDC01

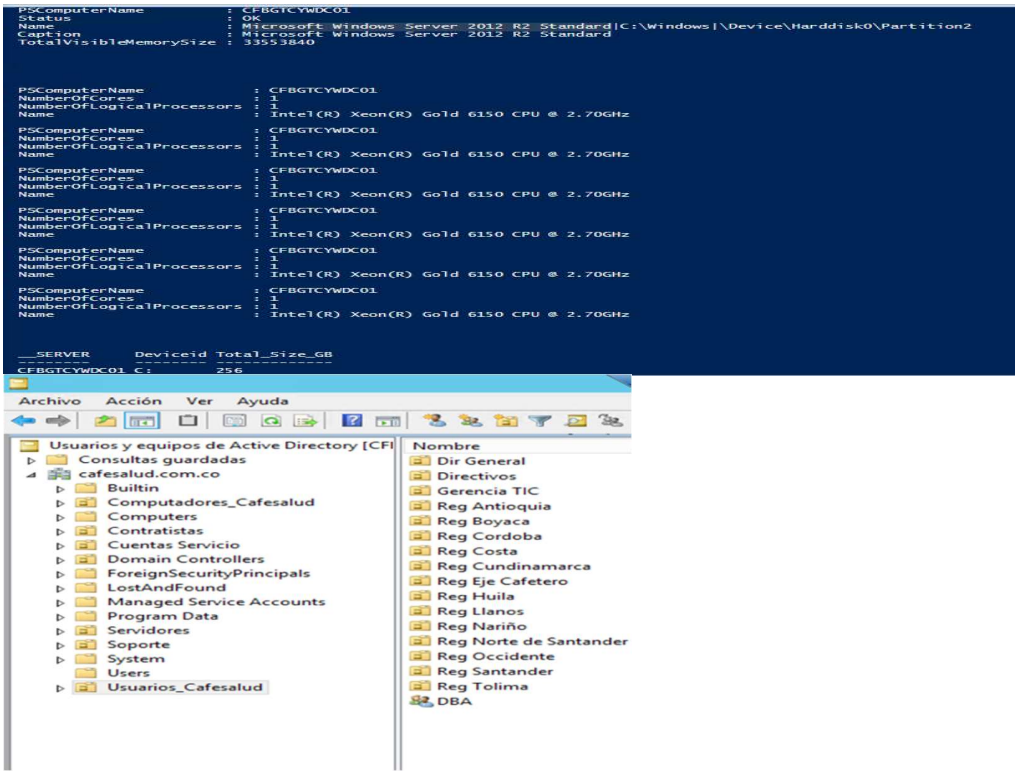
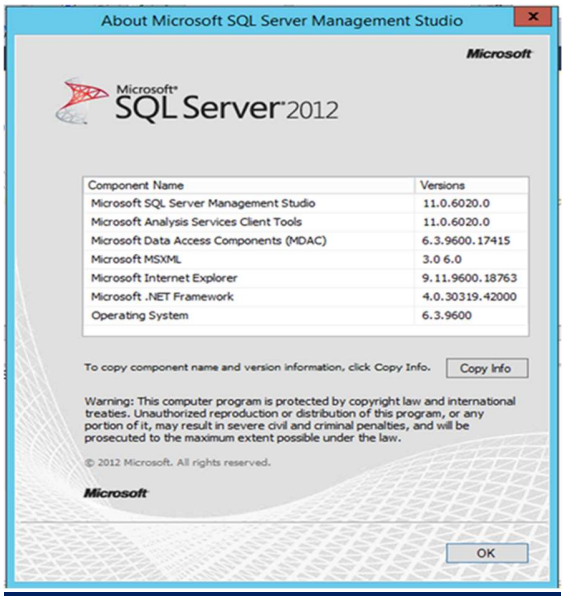


Figura 1 - 7 Evidencia de inventario de servidores CFBGTCYWDC01

CFBGTCYWDBS01



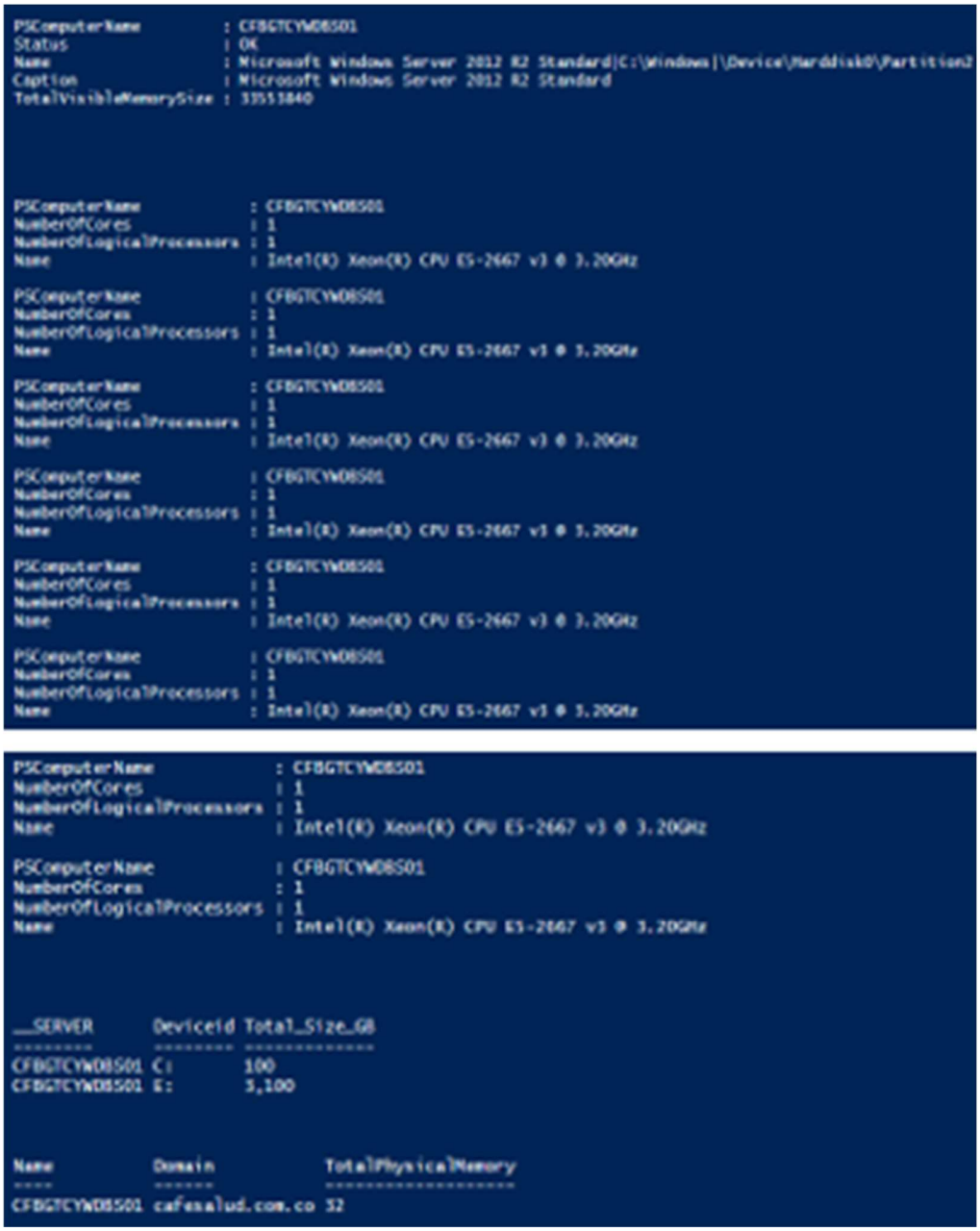
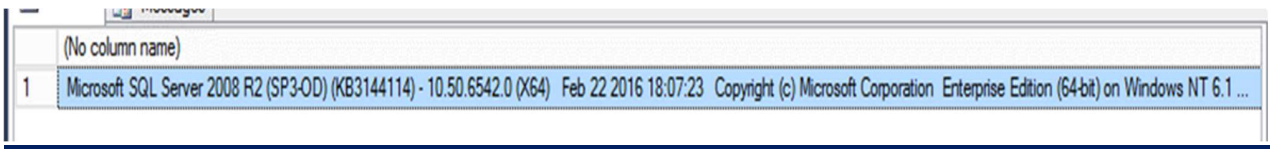


Figura 1 - 8 Evidencia de inventario de servidores CFBGTCYWDBS01

ADMINISTRAR



	(No column name)
1	Microsoft SQL Server 2008 R2 (SP3-OD) (KB3144114) - 10.50.6542.0 (X64) Feb 22 2016 18:07:23 Copyright (c) Microsoft Corporation Enterprise Edition (64-bit) on Windows NT 6.1 ...

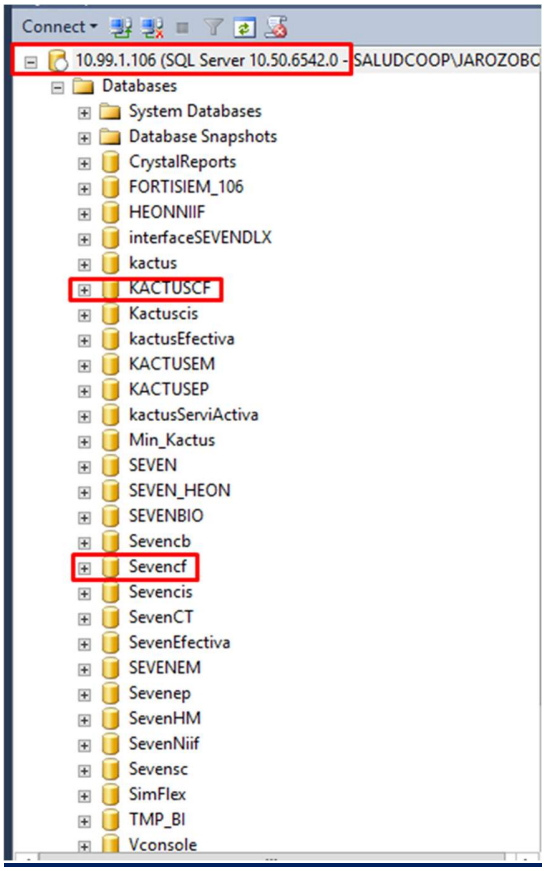


Figura 1 - 9 Evidencia de inventario de servidores ADMINISTRAR

SEVENCFHN01

```
Status                : OK
Name                  : Microsoft Windows Server 2008 R2 Enterprise |C:\Windows|\Device\Harddisk0\Partition2
Caption               : Microsoft Windows Server 2008 R2 Enterprise
TotalVisibleMemorySize : 8388152



PS C:\Users\jarozobo> Get-WmiObject -Class Win32_Processor -ComputerName . | Format-List PSComputerName,NumberOfCores, N
umberOfLogicalProcessors,Name


NumberOfCores             : 4
NumberOfLogicalProcessors : 4
Name                      : Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz



PS C:\Users\jarozobo> gwmi -class "win32_LogicalDisk" -computername  $hots_name | where{$_.DriveType -like "3"} | ft __S
ERVER,Deviceid,@{expression={"{0:N0}" -f ($_.Size/1GB)};label="Total_Size_GB"} -auto

__SERVER    Deviceid Total_Size_GB
--------    -------- -------------
SEVENCFHN01 C:       46
SEVENCFHN01 D:       409


PS C:\Users\jarozobo> Get-WmiObject Win32_ComputerSystem -ComputerName . | Format-Table Name,Domain,@{expression={"{0:N0
}" -f (($_.TotalPhysicalMemory/1GB))};label="TotalPhysicalMemory"}

Name                                Domain                              TotalPhysicalMemory
----                                ------                              -------------------
SEVENCFHN01                         saludcoop.com.co                    8
```

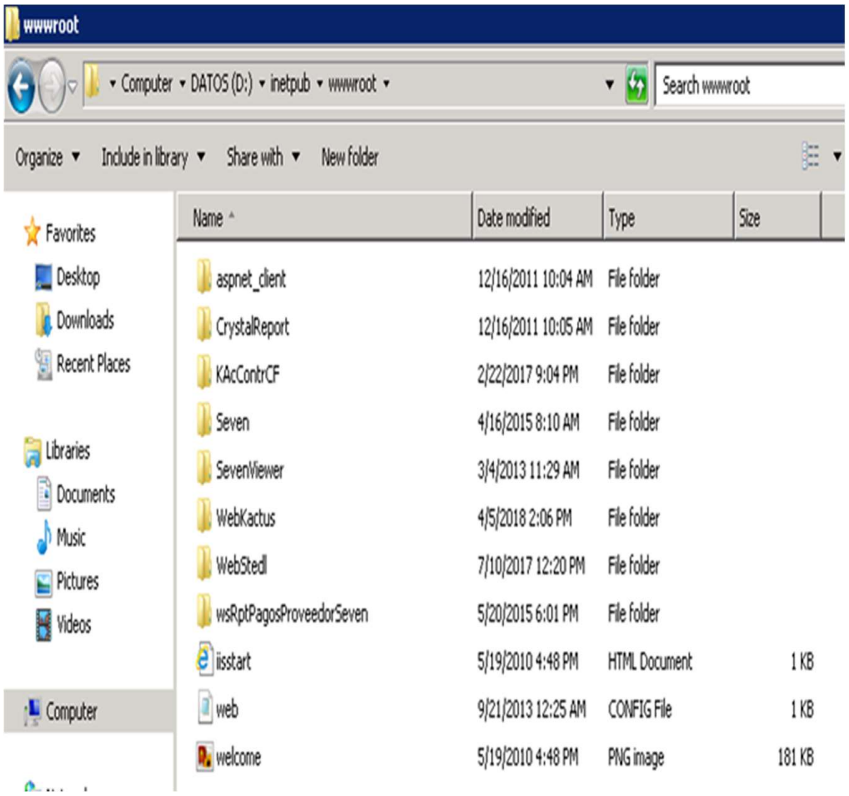
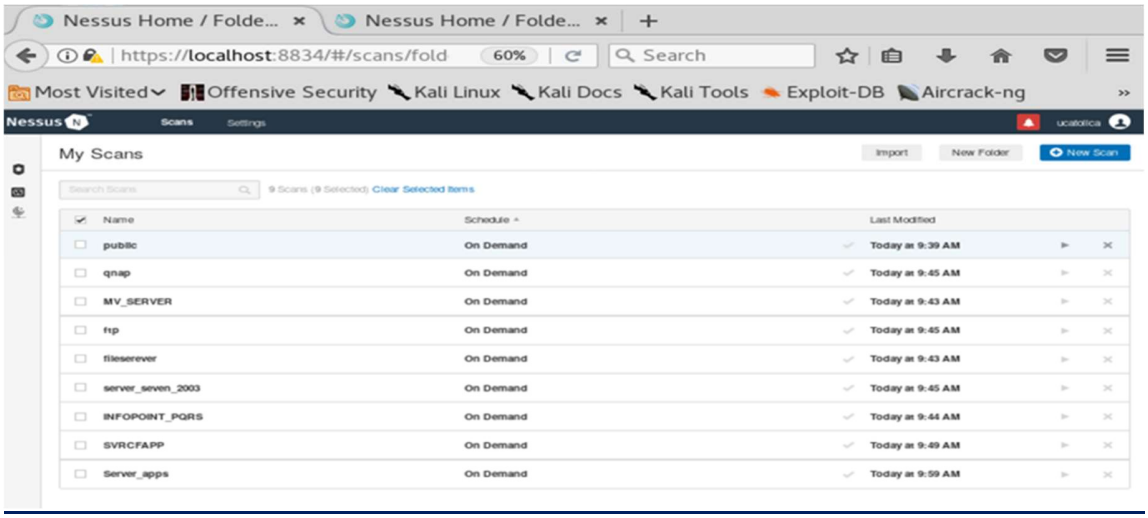


Figura 1 - 10 Evidencia de inventario de servidores SEVENCFHN01

En este capítulo se desarrolla el segundo objetivo planteado, se detectan y analizan las vulnerabilidades de los principales servidores

SERVER SVRCFAPP →10.127.209.221



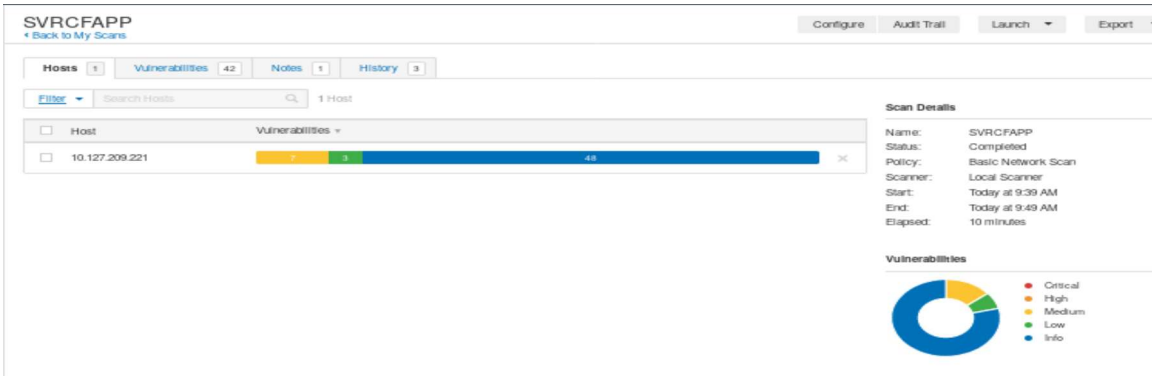


Figura 1 - 11 Vulnerabilidades SERVER SVRCFAPP 10.127.209.221

SERVER_SEVEN_2003 →10.127.209.229

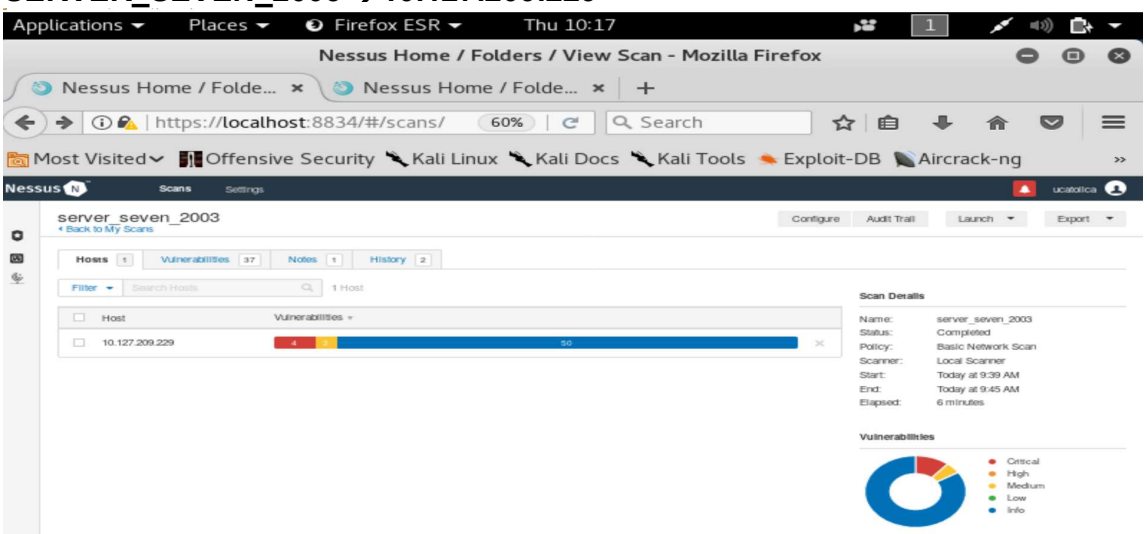


Figura 1 - 12 Vulnerabilidades SERVER_SEVEN_2003 10.127.209.229

QNAP DISPOSITIVO DE ALMACENAMIENTO→10.26.9.219

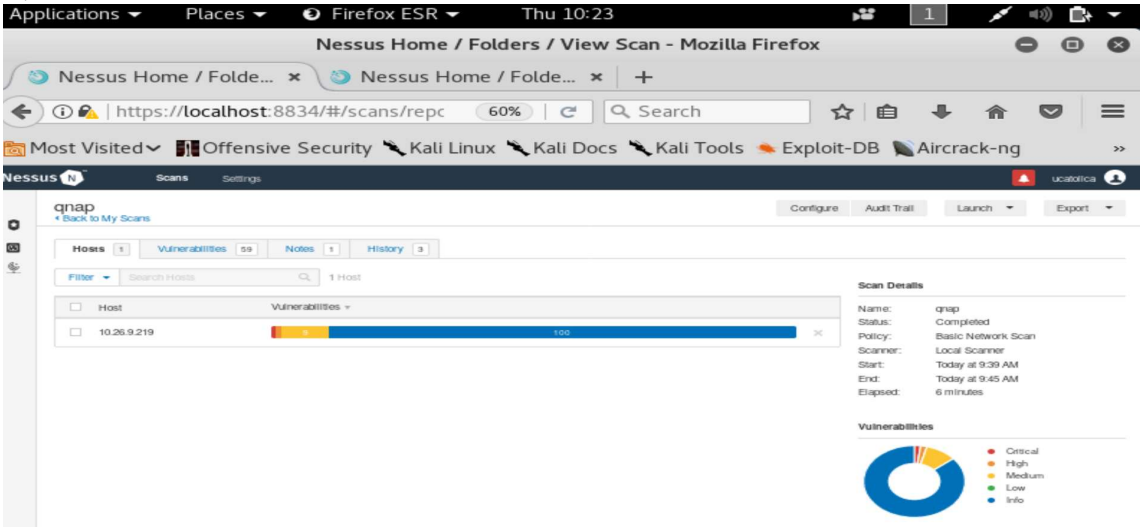


Figura 1 - 13 Vulnerabilidades QNAP DISPOSITIVO DE ALMACENAMIENTO 10.26.9.219

FTP SERVER →10.127.209.126

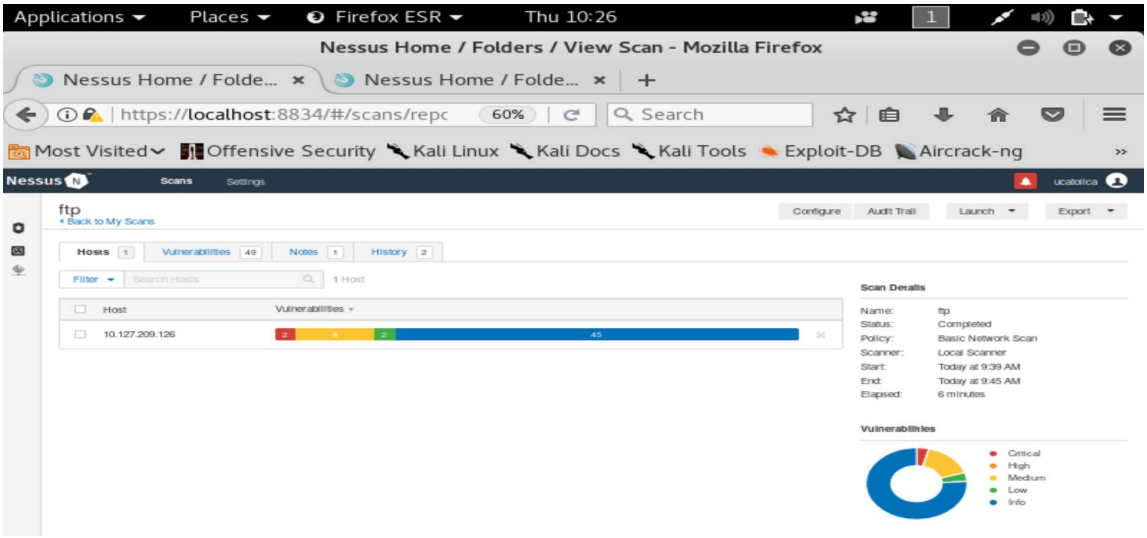


Figura 1 - 14 Vulnerabilidades FTP SERVER 10.127.209.126

INFOPOINT PQRS → 10.127.209.220

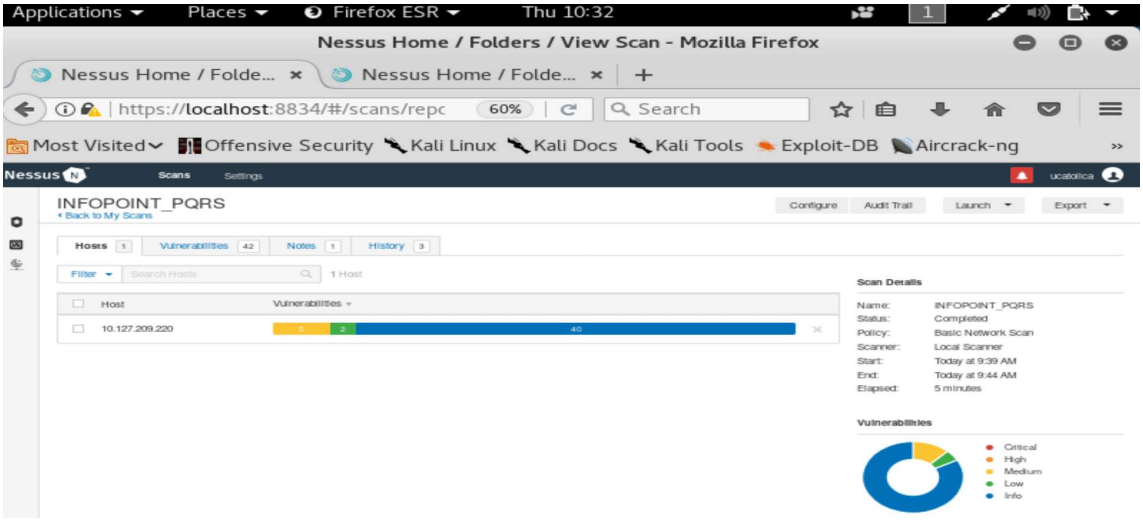


Figura 1 - 15 Vulnerabilidades INFOPOINT PQRS 10.127.209.220

SERVIDOR HOST PRINCIPAL →10.127.209.160

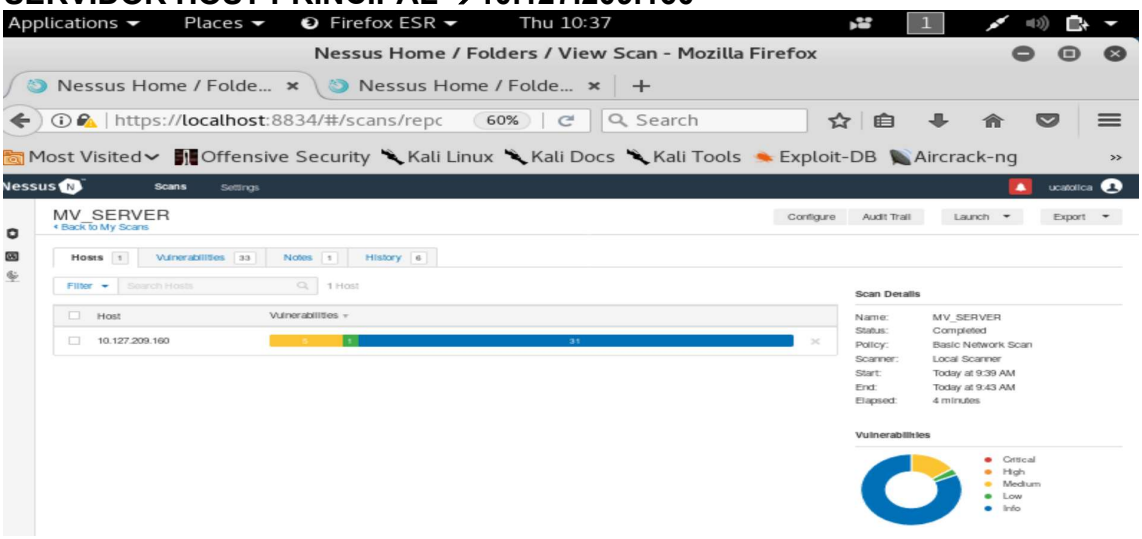


Figura 1 - 16 Vulnerabilidades SERVIDOR HOST PRINCIPAL 10.127.209.160

SERVER FILE SERVER → 10.26.7.230

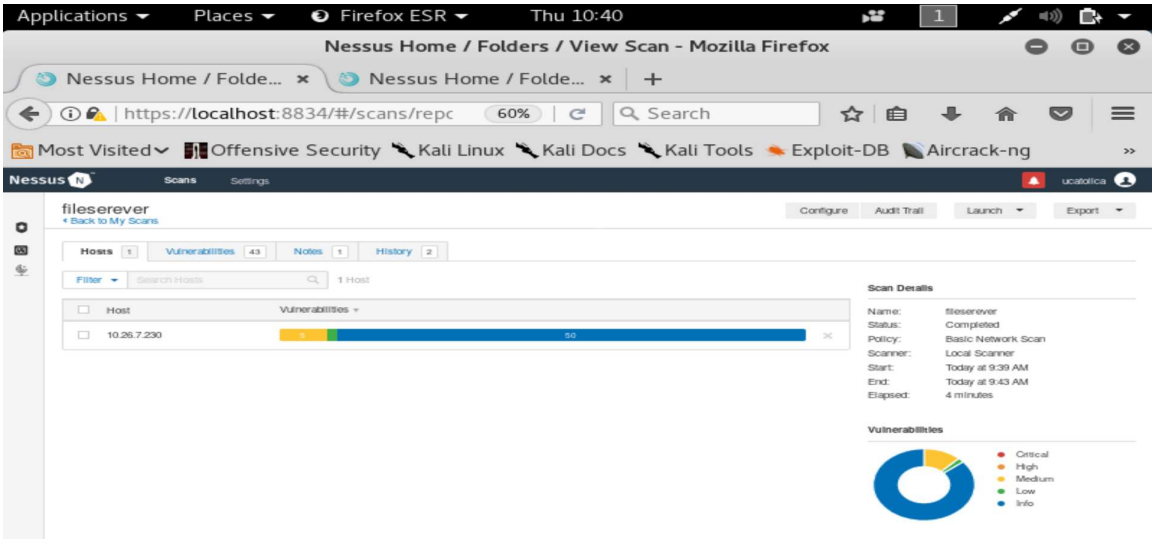


Figura 1 - 17 Vulnerabilidades SERVER FILE SERVER 10.26.7.230

Las vulnerabilidades en los sistemas operativos pueden conducir al acceso no autorizado a datos y la corrupción. Revisamos 10 IP (Servidores) donde encontramos 70 vulnerabilidades entre las cuales 12 fueron bajas, 49 medias y 9 altas, se encontró que una vulnerabilidad puede repetirse en diferentes servidores a continuación mostramos la información consolidada de las vulnerabilidades Y la Torta con los porcentajes alto, medio y bajo.

Detención de Vulnerabilidades

Vulnerabilidades totales	
Grado	Cantidad
Alto	9
Medio	49
Bajo	12

Servidor	Alto	Medio	Bajo
10.127.209.229	4	2	0
10.127.209.116	2	7	2
10.26.9.219	2	6	0
10.127.209.126	1	8	2
10.127.209.221	0	6	3
10.127.209.220	0	5	2
10.26.7.230	0	5	1
10.127.209.84	0	5	1
10.127.209.160	0	5	1
10.127.209.81	0	0	0

Figura 1 - 18 Vulnerabilidades totales

En el anexo 1 encontramos la información sobre las vulnerabilidades encontradas donde podemos ver el nombre de la vulnerabilidad, su descripción , el factor de riesgo, las maquinas afectadas, en que grado de vulnerabilidad se encuentran, los servicios que se están afectando y colocamos una posible solución para mitigar el riesgo de la vulnerabilidad.

Para mitigar y dar solución a estas vulnerabilidades que por lo visto se genera en varias máquinas se sugiere:

- Impedir acceso a archivos desde navegador.
- Desactivar los algoritmos de cifrado débiles
- Filtrar el tráfico generado por los puertos más vulnerables.
- Reemplazar certificados SSL vencidos por nuevos.
- Desactivar páginas predeterminadas dentro de la configuración del servidor.
- Desactivar protocolos de cifrado SSLv2 y SSLv3 obsoletos, utilizar TLSv1 +.
- Actualizar versión de PHP
- Utilizar contraseñas con nivel de seguridad alto, además de cambiarlas periódicamente.
- Actualización y divulgación de las políticas de Seguridad de la Información.

- Configurar el servicio NFS para que únicamente permita la conexión de equipos autorizados.
- Aplicar las actualizaciones publicadas por Microsoft en el boletín de seguridad MS14-066.
- Aplicar las actualizaciones publicadas por Microsoft en el boletín de seguridad MS15-034.
- Realizar una migración de los servicios a un sistema operativo con soporte por parte del desarrollador.
- Forzar el uso de SSL como capa de transporte de datos del servicio de escritorio remoto y habilitar la opción 'Permitir conexiones solo de equipos que ejecuten Escritorio remoto con Autenticación a nivel de red' Mayor información: https://technet.microsoft.com/es-co/library/cc732713.aspx
- Restringir el acceso anónimo al equipo en las conexiones remotas del servicio de escritorio remoto.
- Obtener un certificado digital nuevo con una firma digital que utilice un algoritmo de hash robusto.
- Coloque las restricciones necesarias para el NFS sobre los directorios
- Cambiar el nivel de cifrado del servicio a Alto o a cumplimiento de FIPS
- Habilitar el uso de la autenticación a nivel de red (NLA) por parte del servicio de escritorio remoto.
- Reconfigure la aplicación afectada para que, en la medida de lo posible, evite el uso de suites de cifrado RC4.
- Reconfigure el servicio para soportar únicamente módulos Diffie-Hellman de al menos 2048 bits.

7.2. IDENTIFICACIÓN DE LOS RIESGOS

Matriz análisis de riesgo

Identificación de riesgos. El proceso de identificación de riesgos estuvo determinado por la identificación y clasificación de los activos. Estos se clasificaron en:

Activos hardware y software. Hacen referencia a los equipos y software utilizados para manejar la información

Activos de Información. Estos activos son unos de los más delicados y vulnerables en la matriz de riesgos, porque son los que van a almacenar y manejar la información de la empresa.

Nombre	IP	Tipo de Servidor	Sistema Operativo	Versión Sistema Operativo	Capa	Aplicaciones
CFBGTCYWDC01	10.127.96.2	VIRTUAL	Windows	Microsoft Windows Server 2012 R2 Standard	AD	ACTIVE DIRECTORY
CFBGTCYWINFOAPP	10.127.96.6	VIRTUAL	Windows	Microsoft Windows Server 2012 R2 Standard	APLICACIÓN	APLICACIÓN INFOPOINT TUTELAS
CFBGTCYWPRWEB01	10.127.96.15	VIRTUAL	Linux	CentOS Linux release 7.3.1611 (Core)	APLICACIÓN	Paginaweb
SEVENCFHN02	10.99.1.17	VIRTUAL	Windows	MicrosoftWindows 2008 R2 Enterprise	APLICACIÓN	Seven
SEVENCFHN01	10.99.1.82	VIRTUAL	Windows	MicrosoftWindows 2008 R2 Enterprise	APLICACIÓN	Seven-Kactus
CRYSTALSEVEN	10.99.1.129	VIRTUAL	Windows	Microsoft Windows Server 2003 Enterprise	APLICACIÓN	Seven Reportes
HEONINFOPATH		VIRTUAL	Windows	MicrosoftWindows 2008 R2 Enterprise	APLICACIÓN	Infopointpqrs
SVRCRPDCF	10.26.9.159	VIRTUAL	Windows	Microsoft Windows Server 2012 Standard	APLICACIÓN	Correspondencia
DACAFESALUDA	10.26.9.215	VIRTUAL	Windows	Microsoft Windows 10 Pro	APLICACIÓN	INTRANET
SVRCF	10.26.9.226	VIRTUAL	Windows	Microsoft Windows Server 2012 Standard	APLICACIÓN	JURIDICA-FINANCIERA-MATRIZ
CFPRODUCCION	10.26.9.216	VIRTUAL	Windows	Microsoft Windows 10 Pro	APLICACIÓN	FINANCIERA
CFBGTCYWDWH01	10.127.96.4	VIRTUAL	Windows	Microsoft Windows Server 2012 R2 Standard	BASE DE DATOS	BD_CAFESALUD
CFBGTCYWINFODB0	10.127.96.5	VIRTUAL	Windows	Microsoft Windows Server 2012 R2 Standard	BASE DE DATOS	BD Infopoint tutelas
CFBGTCYWDBS01	10.127.96.10	VIRTUAL	Windows	Microsoft Windows Server 2012 R2 Standard	BASE DE DATOS	BD Operaciones y afiliaciones
CFBGTCYWATDBBK02	10.127.96.14	VIRTUAL	Windows	Micrsoft Windows 2000 Service Pack 4	BASE DE DATOS	Aletheia
ADMINISTRAR	10.99.1.106	VIRTUAL	Windows	MicrosoftWindows 2008 R2 Enterprise	BASE DE DATOS	Seven-Kactus
CRUXBLANCA	19.99.1.115	VIRTUAL	Windows	MicrosoftWindows 2008 R2 Enterprise	BASE DE DATOS	Infopointpqrs
CAFESALUD	10.99.1.114	VIRTUAL	Windows	MicrosoftWindows 2008 R2 Enterprise	BASE DE DATOS	Cuentas Medicas -Habilitar -Prestar
SVRCRPDBDCF	10.26.9.158	VIRTUAL	Windows	Microsoft Windows Server 2012 R2 Data Center	BASE DE DATOS	Correspondencia
CFBGTCYWFIL01	10.127.96.11	VIRTUAL	Windows	Microsoft Windows Server 2012 R2 Standard	FTP	FTP
SVRTICSCFMV	10.26.9.224	FISICO	Windows	Microsoft Windows Server 2012 R2 Data Center	Host	HOST FISICO
SVRTICSCF	10.26.9.223	VIRTUAL	Windows	Microsoft Windows Server 2012 R2 Data Center	Host	HOST FISICO

Figura 1 - 19 Inventario de activos de servidores con especificaciones

ANÁLISIS DE RIESGO

Habiendo ya identificado las vulnerabilidades que hay en los activos de la EPS en liquidación, pasamos a revisar los riesgos y su análisis, es decir, se estudian la posibilidad y las consecuencias de cada factor de riesgo, el análisis de los riesgos determinará cuáles son los factores de riesgo que potencialmente tendrían un mayor efecto sobre la Eps en Liquidación y, por lo tanto, deben ser gestionados con especial atención.

Identificación y clasificación de Riesgos y Amenazas. Estas fueron identificadas y clasificadas de la manera:

AMENAZAS EN LOS ACTIVOS FISICOS (SERVIDORES)
Pérdida de información
Robo de equipos
Virus
Robo de medios
Destrucción o daño de equipos

AMENAZAS SOBRE APLICACIONES
Pérdida de información
Abuso de derechos
Divulgación no autorizada de la información
Falla de las aplicaciones críticas
Virus
Modificación no autorizada de la información
Robo de información
Divulgación de la información

AMENAZAS SOBRE LA RED
Robo de información
Indisponibilidad de la red
Destrucción o daño de equipos

Escogimos metodología de evaluación de la criticidad pues esta evalúa activos y como pueden impactar a la empresa.

Criticidad

CUALITATIVA				CUANTITATIVA		
VALOR	NIVEL	CRITERIOS		VALOR	NIVEL	CRITERIOS
5	MUY ALTO	La pérdida de Integridad, Disponibilidad y Confidencialidad del activo, impacta negativamente tanto las finanzas y la reputación de la entidad.		5	MUY ALTO	Mayor o igual a 39 activos
4	ALTO	La pérdida de Integridad, Disponibilidad y Confidencialidad del activo, impacta negativamente la reputación de la entidad.		4	ALTO	Mayor o igual a 29 activos
3	MEDIO	La pérdida de Integridad, Disponibilidad y Confidencialidad del activo, impacta negativamente las finanzas de la entidad.		3	MEDIO	Mayor o igual a 19 activos
2	BAJO	La pérdida de Integridad, Disponibilidad y Confidencialidad del activo, impacta negativamente a nivel operacional la entidad.		2	BAJO	Mayor o igual a 9 activos
1	MUY BAJO	La pérdida de Integridad, Disponibilidad y Confidencialidad del activo, no genera impacto alguno para la entidad.		1	MUY BAJO	Mayor o igual a 0 activos

Figura 1 - 20 Valores de criticidad

De esta forma se evalúa cada uno de los servidores y demás equipos que componen nuestro centro de datos, utilizando como estándar la **matriz de criticidad** indicada en la siguiente tabla, la cual contiene: el número de activos y el valor criticidad tanto cualitativamente como cuantitativamente y el total del nivel de criticidad el cual sale de la suma de los cualitativos + cuantitativos tanto de las vulnerabilidades como de las amenazas.

MATRIZ DE RIESGOS									
Tipo de Soporte	Subtipo de Soporte	Número de activos	Vulnerabilidades	Criticidad cualitativa	Criticidad cuantitativa	Amenazas	Criticidad cualitativa	Criticidad cuantitativa	Nivel de Criticidad
HARDWARE	Servidor	26	Ausencia de controles de seguridad sobre cada servidor	4	3	Pérdida de información	4	3	14
	Servidor	26	Ausencia de respaldo para archivos en PC	5	3	Pérdida de información	4	3	15
	Servidor	26	Ausencia de entrenamiento en creación de contraseñas seguras	5	3	Robo de información	3	3	14
	Servidor	26	Copia no controlada	5	3	Hurto de medios o documentos	4	3	15
	Dispositivo Móvil	1	Uso de portátiles sin la suficiente protección adecuada fuera de las instalaciones	5	1	Robo de equipos	5	1	12
	Medio extraíble	14	Uso de USB y discos duros externos sin la protección adecuada	5	2	Robo de medios	3	2	12
SOFTWARE	Aplicación	10	No se cuenta con un sistema de Logs (registro) centralizado	3	2	Pérdida de información	4	2	11
	Aplicación	10	Uso incorrecto de softw are	3	2	Abuso de derechos	4	2	11
	Aplicación	10	Ausencia de procedimientos formales y usados para el desarrollo seguro	3	2	Divulgación no autorizada de la información	5	2	12
	Aplicación	10	Ausencia de estándares de configuración	2	2	Falla de la aplicaciones críticas	4	2	10
	Ofimática	7	No respaldo de información digital importante	5	1	Virus	4	1	11
	Base de datos	8	Ausencia de estándares de configuración en la Base de datos	4	1	Indisponibilidad de la base de datos	5	1	11
	Base de datos	8	Configuración insegura de la Base de datos	5	1	Modificación no autorizada de la información	5	1	12
	Sistema operativo	1	Ausencia de revisión periódica de permisos de usuarios en los sistemas (file servers)	4	1	Robo de información	5	1	11
	E-MAIL	32	Uso de correos personales sin medidas adecuadas de seguridad	4	4	Divulgación no autorizada de la información	4	4	16
REDES	Red Pública	0	Uso inseguro de tecnologías de almacenamiento en la nube	2	1	Robo de información	5	1	9
	WAN Privada	32	falta de controles de supervisión de la red WAN privada	2	4	Indisponibilidad de la red	3	4	13
	LAN	8	No se realiza gestión de la capacidad en la red	2	1	Indisponibilidad de la red	3	1	7
	LAN	8	No se realiza gestión de la disponibilidad en la red	2	1	Indisponibilidad de la red	3	1	7
	LAN	8	No registro de logs de los dispositivos de red	3	1	Indisponibilidad de la red	3	1	8
	Datacenter	1	Ausencia de control formal sobre condiciones ambientales en Datacenter	3	1	Pérdida de servicios esenciales	5	1	10
	Datacenter	1	Ausencia de planta generadora alterna	3	1	Falla de potencia	3	1	8
	Archivo de gestión	26	Ubicación no segura del archivo físico	4	3	Daño físico en documentos	3	3	13
	Archivo de gestión	26	Ausencia de control formal sobre condiciones ambientales en archivo	3	3	Daño físico en documentos	3	3	12
	Archivo de gestión	26	No respaldo de información física importante	5	3	Pérdida de información	4	3	15
	Archivo de gestión	26	Ausencia de controles físicos para evitar sustracciones o pérdida de carpetas	5	3	Pérdida de información	3	3	14
PERSONAL	Personal Interno	35	Falta de socialización en las políticas de seguridad de la información	5	4	Robo de información	5	4	18
	Personal Interno	35	no se realiza control sobre la politica de Escritorio limpio	5	4	Uso no autorizado de equipos	5	4	18
	Personal Interno	35	Insuficientes controles de acceso	5	4	Planes de Continuidad del negocio	5	4	18
	Personal Interno	35	Ausencia de sensibilización en el uso correcto de los procedimientos	5	4	Fallas en la operación	5	4	18
	Personal Interno	35	Insuficiente entrenamiento para la creación de contraseñas	5	4	Robo de información	5	4	18
	Personal Externo	3	Falta de sensibilización de seguridad de la información	5	1	Robo de información	5	1	12
PROCEDIMENTAL Y ESTRUCTURAL	Políticas	3	Ausencia de políticas para el uso de criptografía	4	1	Modificación no autorizada de la información	5	1	11
	Políticas	3	Ausencia de políticas para el borrado seguro y eliminación de equipos	3	1	Copia fraudulenta de información	5	1	10
	Políticas	3	No se realiza revisión de documentos de seguridad de la información	3	1	Divulgación no autorizada de la información	4	1	9
	Políticas	3	Ausencia de manual para asignar roles y responsabilidades	4	1	Divulgación no autorizada de la información	4	1	10
	Políticas	3	Política para el uso de controles criptográficos	4	1	Divulgación no autorizada de la información	4	1	10
	Procedimientos	3	Ausencia de estándares de configuración para TI	4	1	Robo de información	5	1	11
	Procedimientos	3	Ausencia de procedimientos para TI	4	1	Indisponibilidad de TI	4	1	10
	Procedimientos	3	No se cuenta con políticas y procedimientos de desarrollo seguro	4	1	Pérdida de información	4	1	10
	Procedimientos	3	No se cuenta con un plan de continuidad del negocio	5	1	Indisponibilidad general de la sede	5	1	12
	Procedimientos	3	Ausencia de auditorias formales y regulares	3	1	Abuso de derechos	4	1	9
	Procedimientos	3	Falta de procedimientos formales para el análisis de vulnerabilidades	4	1	Robo de información	5	1	11
	Procedimientos	3	Ausencia de procedimientos para la gestión de incidentes de seguridad	5	1	Pérdida de información	5	1	12
	Procedimientos	3	Ausencia de políticas y procedimientos para la transferencia de información	5	1	Escucha fraudulenta	5	1	12
	Procedimientos	3	Ausencia de políticas y procedimientos para los datos de prueba	3	1	Copia fraudulenta de información	5	1	10

Figura 1 - 21 Matriz de valoración

Las amenazas para detectar los riesgos las escogimos de el nivel de criticidad identificado de 10 a 20

Amenazas	Nivel de Criticidad
Falla de las aplicaciones críticas	10
Pérdida de servicios esenciales	10
Copia fraudulenta de información	10
Divulgación no autorizada de la información	10
Indisponibilidad de TI	10
Pérdida de información	10
Abuso de derechos	11
Virus	11
Indisponibilidad de la base de datos	11
Robo de información	11
Modificación no autorizada de la información	11
Robo de equipos	12
Robo de medios	12
Daño físico en documentos	12
Indisponibilidad general de la sede	12
Escucha fraudulenta	12
Indisponibilidad de la red	13
Hurto de medios o documentos	15
Uso no autorizado de equipos	18
Planes de Continuidad del negocio	18
Fallas en la operación	18

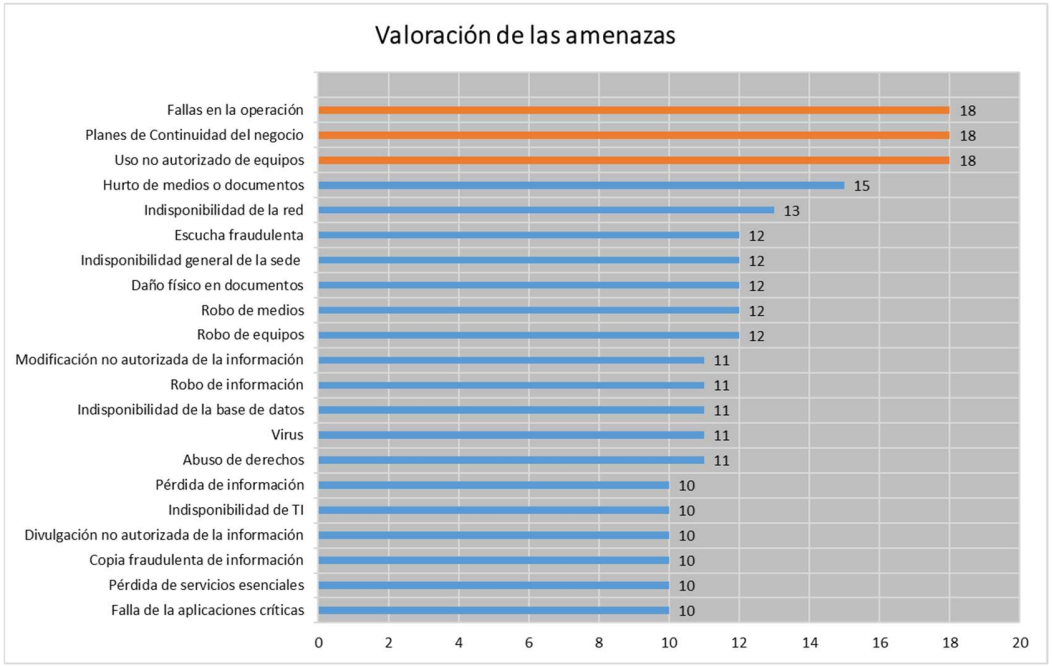


Figura 1 - 22 Valoración de las amenazas

Revisamos matriz para los riesgos inherentes, el riesgo actual que es con los controles que tienen y el riesgo residual que es con los controles propuestos.

Medición	PROBABILIDAD	
5	CASI SEGURO	- Casi con certeza se espera la ocurrencia del evento. - Por lo menos mensual o con mayor frecuencia - Ocurrirá en la mayoría de las circunstancias.
4	PROBABLE	- Significativa probabilidad de ocurrencia. - Anualmente. - Probablemente ocurra en cualquier momento.
3	POSIBLE	- Mediana probabilidad de ocurrencia. - Una vez cada 3 años.
2	IMPROBABLE	- Baja probabilidad de ocurrencia - Una vez cada 5 años
1	RARO	- Muy baja probabilidad de ocurrencia - En 10 años o más - Insignificante - puede ocurrir sólo en circunstancias excepcionales

ESCALA	IMPACTO	
Mayor o igual a 14	Catastrófico	La pérdida de Integridad, Disponibilidad y Confidencialidad causada por el escenario, impacta negativamente tanto las finanzas y la reputación de la entidad.
Entre 12 y 13	Alto	La pérdida de Integridad, Disponibilidad y Confidencialidad causada por el escenario, impacta negativamente la reputación de la entidad.
Entre 8 y 11	Moderado	La pérdida de Integridad, Disponibilidad y Confidencialidad causada por el escenario impacta negativamente las finanzas de la entidad.
Entre 3 y 7	Menor	La pérdida de Integridad, Disponibilidad y Confidencialidad causada por el escenario, impacta negativamente a nivel operacional la entidad.
Menor a 3	Insignificante	La pérdida de Integridad, Disponibilidad y Confidencialidad causada por el escenario, no genera impacto alguno para la entidad.

RIESGO

PROBABILIDAD	IMPACTO				
	Insignificante (3)	Menor (6)	Moderado (9)	Mayor (12)	Catastrófico (15)
Casi seguro (5)	15	30	45	60	75
Probable (4)	12	24	36	48	60
Posible (3)	9	18	27	36	45
Improbable (2)	6	12	18	24	30
Raro (1)	3	6	9	12	15

NIVEL DE RIESGO	DESCRIPCIÓN DEL RIESGO
Extremo	Si una situación se evalúa como de extremo riesgo, hay una necesidad inminente y urgente de tomar medidas correctivas en el corto plazo. El sistema puede continuar funcionando, pero se debe realizar cuanto antes un plan de acción correctiva.
Alto	Si una situación se evalúa como de alto riesgo, hay una necesidad inminente de tomar medidas correctivas en el corto o mediano plazo.
Moderado	Si una situación se clasifica como de riesgo moderado, las acciones correctivas son necesarias y se debe desarrollar un plan para incorporar estas acciones dentro de un período de tiempo razonable.
Bajo	Si una situación se clasifica como de riesgo bajo, debe decidirse si las acciones correctivas son requeridas o se acepta el riesgo.

Figura 1 - 23 Valorares probabilidad, impacto y riesgo

ID	Riesgos	RIESGO INHERENTE			APLICACIÓN Y EFICACIA DE CONTROLES EXISTENTES		RIESGO RESIDUAL		
		Probabilidad	Impacto	Riesgo	Controles Existentes	Eficacia del control	Probabilidad	Impacto	Riesgo
1	**Falla de la aplicaciones críticas**	Raro	Mayor	Alto	Se cuenta con personal calificado en el manejo y desarrollo de aplicaciones	Media	Raro	Mayor	Alto
2	**Pérdida de servicios esenciales**	Raro	Moderado	Moderado	Entrenamiento en las diferentes aplicaciones	Media	Raro	Moderado	Moderado
3	**Copia fraudulenta de información**	Improbable	Moderado	Moderado	Controles de acceso lógicos (firewall, antivirus y credenciales)	Media	Improbable	Moderado	Moderado
4	**Divulgación no autorizada de la información**	Improbable	Moderado	Moderado	Controles de acceso lógicos (firewall, antivirus y credenciales)	Media	Improbable	Moderado	Moderado
5	**Indisponibilidad de TI**	Posible	Moderado	Alto	Personal calificado y mantenimientos preventivos	Media	Posible	Moderado	Alto
6	**Pérdida de información**	Posible	Moderado	Alto	Directorio activo configurado de manera segura	Media	Posible	Moderado	Alto
7	**Abuso de derechos**	Improbable	Moderado	Moderado	Control de acceso lógico y directorio activo	Media	Improbable	Moderado	Moderado
8	**Virus**	Posible	Mayor	Extremo	Antivirus y actualizaciones de software	Alta	Posible	Moderado	Alto
9	**Indisponibilidad de la base de datos**	Improbable	Moderado	Moderado	Entrenamiento en los diferentes sistemas	Media	Improbable	Moderado	Moderado
10	**Robo de información**	Raro	Mayor	Alto	Controles de acceso lógicos (firewall, antivirus y credenciales)	Media	Raro	Mayor	Alto
11	**Modificación no autorizada de la informació**	Raro	Moderado	Moderado	Contraseñas y controles de acceso lógico	Media	Raro	Moderado	Moderado
12	**Robo de equipos**	Posible	Moderado	Alto	Controles de acceso físico	Media	Posible	Moderado	Alto
13	**Robo de medios**	Posible	Moderado	Alto	Controles de acceso físico	Media	Posible	Moderado	Alto
14	**Daño físico en documentos**	Posible	Mayor	Extremo	Controles de acceso físico	Media	Posible	Mayor	Extremo
15	**Indisponibilidad general de la sede**	Raro	Mayor	Alto	Mantenimientos preventivos y controles de acceso físico	Media	Raro	Mayor	Alto
16	**Escucha fraudulenta**	Improbable	Moderado	Moderado	Segmentación de redes y cuarto de cableado protegido	Media	Improbable	Moderado	Moderado
17	**Indisponibilidad de la red**	Improbable	Mayor	Alto	Sistemas de alto desempeño y confiabilidad	Alta	Improbable	Moderado	Moderado
18	**Hurto de medios o documentos**	Improbable	Moderado	Moderado	Controles de acceso físico	Media	Improbable	Moderado	Moderado
19	**Uso no autorizado de equipos**	Improbable	Mayor	Alto	Directorio activo configurado de manera segura	Media	Improbable	Mayor	Alto
20	**Planes de Continuidad del negocio**	Raro	Catastrófico	Alto	Se realiza entrenamiento en los diferentes sistemas para la continuidad	Media	Raro	Catastrófico	Alto
21	**Fallas en la operación**	Improbable	Catastrófico	Extremo	Entrenamiento en los diferentes sistemas	Media	Improbable	Catastrófico	Extremo

Tabla 1 - 2 Matriz de riesgo

ID	Riesgos	EVALUACION DE CONTROLES RECOMENDADOS				RIESGO DESPUES DE MITIGACION
		CONTROL RECOMENDADO ANEXO A ISO 27001	Eficacia esperada del control	Probabilidad	Impacto	Riesgo
1	**Falla de las aplicaciones críticas**	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Alta	Raro	Moderado	Moderado
2	**Pérdida de servicios esenciales**	17.1.2 Implantación de la continuidad de la seguridad de la información.	Alta	Raro	Menor	Bajo
3	**Copia fraudulenta de información**	12.3.1 Copias de seguridad de la información.	Alta	Improbable	Menor	Bajo
4	**Divulgación no autorizada de la información**	6.1.1 Asignación de responsabilidades para la seguridad de la información.	Alta	Improbable	Menor	Bajo
5	**Indisponibilidad de TI**	17.1.1 Planificación de la continuidad de la seguridad de la información.	Alta	Posible	Menor	Moderado
6	**Pérdida de información**	12.3.1 Copias de seguridad de la información.	Alta	Posible	Menor	Moderado
7	**Abuso de derechos**	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Alta	Posible	Menor	Moderado
8	**Virus**	12.2.1 Controles contra el código malicioso.	Media	Probable	Moderado	Alto
9	**Indisponibilidad de la base de datos**	14.2.2 Procedimientos de control de cambios en los sistemas.	Alta	Improbable	Menor	Bajo
10	**Robo de información**	16.1.1 Responsabilidades y procedimientos.	Alta	Raro	Moderado	Moderado
11	**Modificación no autorizada de la información**	9.4.1 Restricción del acceso a la información.	Media	Posible	Moderado	Alto
12	**Robo de equipos**	8.1.1 Inventario de activos.	Media	Posible	Moderado	Alto
13	**Robo de medios**	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Media	Posible	Moderado	Alto
14	**Daño físico en documentos**	12.3.1 Copias de seguridad de la información.	Alta	Posible	Moderado	Alto
15	**Indisponibilidad general de la sede**	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Alta	Raro	Moderado	Moderado
16	**Escucha fraudulenta**	11.2.3 Seguridad del cableado.	Alta	Improbable	Menor	Bajo
17	**Indisponibilidad de la red**	13.1.1 Controles de red.	Alta	Posible	Menor	Moderado
18	**Hurto de medios o documentos**	11.1.2 Controles físicos de entrada.	Alta	Improbable	Menor	Bajo
19	**Uso no autorizado de equipos**	12.6.2 Restricciones en la instalación de software.	Alta	Improbable	Moderado	Moderado
20	**Planes de Continuidad del negocio**	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Alta	Raro	Mayor	Alto
21	**Fallas en la operación**	17.1.1 Planificación de la continuidad de la seguridad de la información.	Alta	Improbable	Mayor	Alto

Tabla 1 - 3 Matriz después de mitigación

7.3. RECOMENDACIONES Y MITIGACIONES DE RIESGOS.

Mitigar riesgos en ISO 27001 y en general el proceso de buscar tratamiento a los riesgos, que durante la fase de evaluación han sido identificados.

Mediante la fase de tratamiento buscamos mitigar riesgos en. Esto consiste en definir los controles para aquellos riesgos que hemos identificados en la evaluación de los mismos, buscando disminuir la probabilidad de que suceda el riesgo o al menos reducir los impactos que pudieran originar.

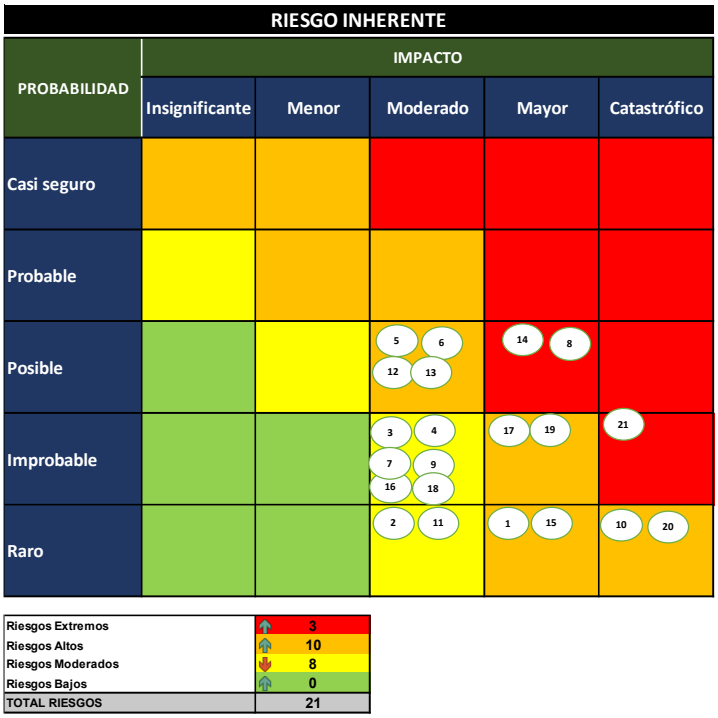
Partiendo de la base de que los recursos disponibles en las organizaciones son limitados, debemos comenzar centrando la atención en aquellos riesgos identificados como no aceptables, de manera que establezcamos un orden de prioridad a la hora de mitigar riesgos.

ID	Riesgos	EVALUACION DE CONTROLES RECOMENDADOS	Aceptabilidad del riesgo	
		CONTROL RECOMENDADO RIESGO ISO 27002		RECOMENDACIÓN
1	**Falla de las aplicaciones críticas**	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Aceptable	El área de Tecnología debe realizar pruebas de todos los sistemas, cuando se presente un cambio de sistema operativo en los equipos de cómputo de la Entidad, con el fin de revisar los posibles impactos en las operaciones o en la seguridad de la información de la organización.
2	**Pérdida de servicios esenciales**	17.1.2 Implantación de la continuidad de la seguridad de la información.	Aceptable	Es necesario proporcionar los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten y que afecten la continuidad de su operación.
3	**Copia fraudulenta de información**	12.3.1 Copias de seguridad de la información.	Aceptable	Se carece de procedimientos formales periódicos de restauración de backups, que incluyan bases de datos con información crítica o sensible.
4	**Divulgación no autorizada de la información**	6.1.1 Asignación de responsabilidades para la seguridad de la información.	Aceptable	Se debe mantener una organización de seguridad, donde los roles y responsabilidades estén definidas y asignadas a los participantes en el modelo de seguridad establecido por la Entidad.
5	**Indisponibilidad de TI**	17.1.1 Planificación de la continuidad de la seguridad de la información.	Aceptable	Se debe desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de la Entidad, sin disminuir los niveles de seguridad establecidos.
6	**Pérdida de información**	12.3.1 Copias de seguridad de la información.	Aceptable	La Entidad certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades
7	**Abuso de derechos**	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Aceptable	La Entidad debe establecer un programa permanente de creación de cultura en seguridad de la información para los empleados y terceros, capacitándolos constantemente en actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
8	**Virus**	12.2.1 Controles contra el código malicioso.	Inaceptable	Verificar y monitorear los controles de restricción al acceso de sitios web que puedan afectar la productividad de los funcionarios aprovechando el Firewall para restringir el acceso y salida a páginas de Internet

9	**Indisponibilidad de la base de datos**	14.2.2 Procedimientos de control de cambios en los sistemas.	Aceptable	El área de Tecnología debe contar con sistemas de control de versiones para restaurar las bases de datos.
10	**Robo de información**	16.1.1 Responsabilidades y procedimientos.	Aceptable	la Entidad promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas
11	**Modificación no autorizada de la información**	9.4.1 Restricción del acceso a la información.	Inaceptable	La asignación de usuarios en los sistemas de información lo deben hacer directamente los lideres o dueños de procesos en la EPS en liquidación
12	**Robo de equipos**	8.1.1 Inventario de activos.	Inaceptable	La Entidad debe mantener un inventario de recursos o activos de información. Los dueños de la información deben clasificar la información basados en su valor, sensibilidad, riesgo de pérdida o compromiso y/o requerimientos legales de retención.
13	**Robo de medios**	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Inaceptable	La Entidad debe establecer un programa permanente de creación de cultura en seguridad de la información para los empleados y terceros, capacitándolos constantemente en actualizaciones regulares sobre las políticas y procedimientos pertinentes en caso de daño, robo o utilizacion de medios.
14	**Daño físico en documentos**	12.3.1 Copias de seguridad de la información.	Inaceptable	La Entidad certificará la generación de copias de respaldo y almacenamiento de su información crítica, e importante teniendo digitalizado sus documentos fisicos importantes
15	**Indisponibilidad general de la sede**	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Aceptable	Se debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.
16	**Escucha fraudulenta**	11.2.3 Seguridad del cableado.	Aceptable	Ubicar el centro de comunicaciones en un sitio seguro y restringido y es necesario que se reciba a satisfacción el cableado y con la respectiva certificación.
17	**Indisponibilidad de la red**	13.1.1 Controles de red.	Aceptable	La Entidad establecerá, a través del área de Tecnología, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas y minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos
18	**Hurto de medios o documentos**	11.1.2 Controles físicos de entrada.	Aceptable	Todas las entradas a las áreas físicas del negocio deben tener un nivel de seguridad acorde con el valor de la información que se procesa y administra en ellas.
19	**Uso no autorizado de equipos**	12.6.2 Restricciones en la instalación de software.	Aceptable	La instalación de software en los computadores suministrados por la Entidad, es una función exclusiva del área de Tecnología y Seguridad de la Información.
20	**Planes de Continuidad del negocio**	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Inaceptable	Debido a que en la EPS en liquidación no se tiene un plan de contingencia se recomienda una vez identificados los procesos, aplicaciones y sistemas que continuarán en funcionamiento, elaborar un instructivo de recuperación oportuno, actualizado y suficientemente probado, que permita garantizar la continuidad del procesamiento de información.
21	**Fallas en la operación**	17.1.1 Planificación de la continuidad de la seguridad de la información.	Inaceptable	se debe desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de la Entidad, sin disminuir los niveles de seguridad establecidos.

Tabla 1 - 4 Matriz de recomendaciones

En los mapas de riesgo podemos ver expresado el riesgo inherente, el riesgo residual y después de mitigación, vemos el total de los riesgos y como quedaron ubicados según el riesgo.



Riesgos Extremos	3
Riesgos Altos	10
Riesgos Moderados	8
Riesgos Bajos	0
TOTAL RIESGOS	21

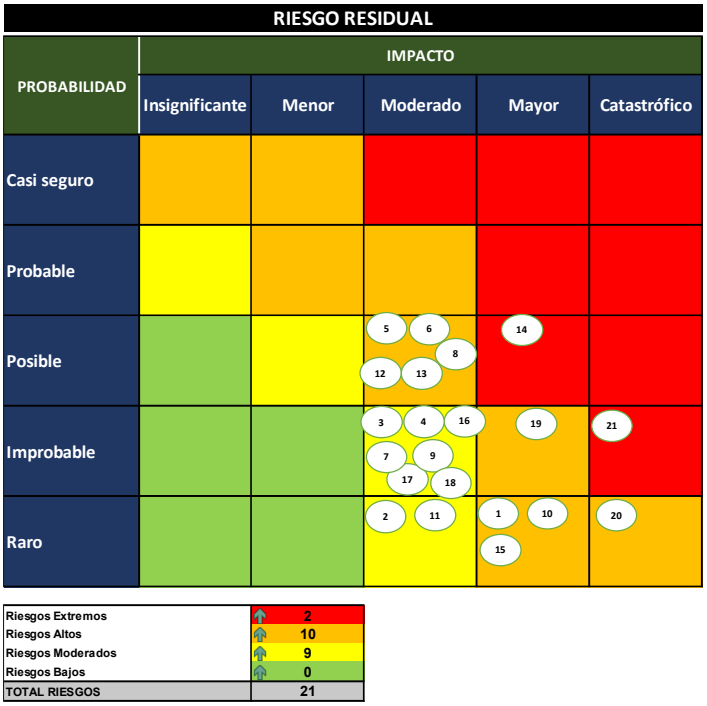
En total medimos 21 riesgos donde podemos ver que en el impacto del R8, R14 y R21 son riesgos extremos donde hay la necesidad inminente y urgente de tomar medidas correctivas en el corto plazo. El sistema puede continuar funcionando, pero se debe realizar cuanto antes un plan de acción correctiva si no sus consecuencias pueden ser catastróficas.
EL R1, R5, R6,R10, R12, R13, R15, R17, R19, Y R20 se encuentran de alto riesgo, hay una necesidad inminente de tomar medidas correctivas en el corto o mediano plazo.

Riesgos Extremos

R8	**Virus**
R14	**Daño físico en documentos**
R21	**Fallas en la operación**

Riesgos Altos

R1	**Falla de las aplicaciones críticas**
R5	**Indisponibilidad de TI**
R6	**Pérdida de información**
R10	**Robo de información**
R12	**Robo de equipos**
R13	**Robo de medios**
R15	**Indisponibilidad general de la sede**
R17	**Indisponibilidad de la red**
R19	**Uso no autorizado de equipos**
R20	**Planes de Continuidad del negocio**



En total medimos 21 riesgos donde podemos ver que en el impacto del R14 y R21 son riesgos extremos donde hay la necesidad inminente y urgente de tomar medidas correctivas en el corto plazo. El sistema puede continuar funcionando, pero se debe realizar cuanto antes un plan de acción correctiva si no sus consecuencias pueden ser catastróficas.
EL R1, R5, R6, R8, R12, R10, R13, R15, R19 y R20 se encuentran de alto riesgo, hay una necesidad inminente de tomar medidas correctivas en el corto o mediano plazo.

Donde vemos que los controles existentes no son suficientes para mitigar los riesgos pues se tienen que tomar medidas correctivas para poder evitar consecuencias que estos riesgos no sean solo amenazas sino que se puedan volver reales.

Riesgos Extremos

R14	**Daño físico en documentos**
R21	**Fallas en la operación**

Riesgos Altos

R1	**Falla de las aplicaciones críticas**
R5	**Indisponibilidad de TI**
R6	**Pérdida de información**
R8	**Virus**
R10	**Robo de información**
R12	**Robo de equipos**
R13	**Robo de medios**
R15	**Indisponibilidad general de la sede**
R19	**Uso no autorizado de equipos**
R20	**Planes de Continuidad del negocio**

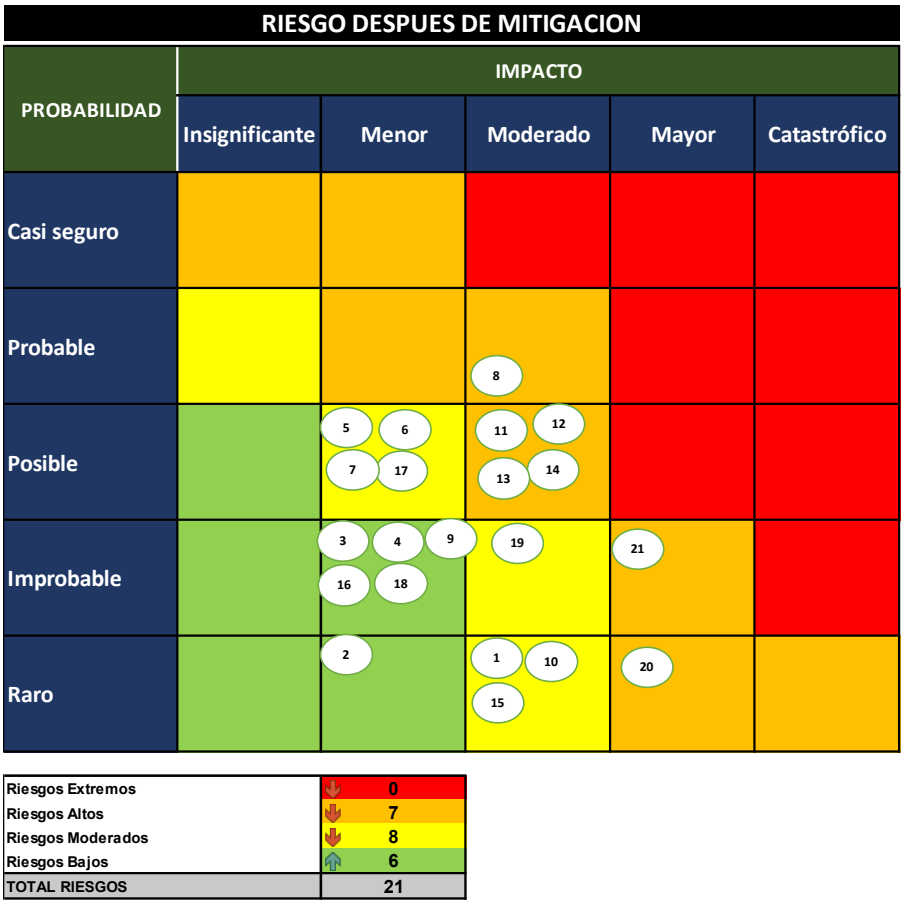


Figura 1 - 24 Mapas de riesgo

En total medimos 21 riesgos donde podemos ver que en el impacto de los riesgos extremos se puede mitigar o minimizar con los controles recomendados

En altos vemos 7 riesgos y ya con el mapa se ve un poco la mitigación de los riesgos a continuación revisamos el resultado del seguimiento de los controles de cuáles fueron las recomendaciones que esta cumplido que no y su respectivo seguimiento.

RESULTADO DEL SEGUIMIENTO.

Calificación del avance.

 No cumplido.

 En ejecución.

 Cumplido.

A continuación, se detalla el resultado obtenido para cada uno de los requerimientos consignados.

Estado	Cantidad	%
Oportunidades de mejora registradas	**15**	**100**
Cumplidas	**6**	**40**
En ejecución	**1**	**7**
No cumplidas	**8**	**53**

Tabla 1 - 5 Estado de la ejecución

RESULTADOS

9. CONTROL DE ACCESOS. **9.1 Requisitos de negocio para el control de accesos.** **9.2 Gestión de acceso de usuario.** **9.4 Control de acceso a sistemas y aplicaciones.**			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
La asignación de usuarios en los sistemas de información lo deben hacer directamente los lideres o dueños de procesos en la EPS en liquidación	De acuerdo con lo informado por el ingeniero a cargo - Ingeniero de Sistemas de la EPS en Liquidación, el proceso de administración de usuarios en los sistemas de información de EPS en Liquidación la están ejecutando correctamente. Para llevar a cabo la asignación de un usuario a los sistemas de información de la entidad, el área de gestión humana de la EPS en liquidación envía un correo electrónico al área de sistemas solicitando la creación de usuarios. Por medio de la mesa de ayuda de, el área de sistemas envía la solicitud para la creación de usuarios con los respectivos perfiles.	La administración de los usuarios, roles y permisos debe estar bajo la responsabilidad del dueño de la información**, EPS en liquidación** en este caso.	

Se debe efectuar un monitoreo y seguimiento de los usuarios activos en los sistemas de información por parte de los dueños o líderes de proceso.	La EPS en liquidación no lleva a cabo monitoreo periódicos sobre los usuarios activos de los sistemas de información de la entidad.	Implementar y/o documentar los procedimientos periódicos de monitoreo sobre los usuarios activos y de las actividades ejecutadas por dichos usuarios.	

Tabla 1 - 6 Control de accesos

12. SEGURIDAD EN LA OPERATIVA **12.1 Responsabilidades y procedimientos de operación** **12.2 Protección contra código malicioso**			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
Verificar y monitorear los controles de restricción al acceso de sitios web que puedan afectar la productividad de los funcionarios aprovechando el Firewall para restringir el acceso y salida a páginas de Internet.	Actualmente EPS en Liquidación no está efectuando un monitoreo de los controles de restricciones de sitios web, no se entrega un informe con indicadores de monitoreo y seguimiento.	Solicitar reportes semanales de monitoreo y seguimiento de la navegación por internet de los usuarios de la EPS en liquidación. (Indicadores de uso de ancho de banda, accesos a Internet, entre otros). Solicitar una herramienta que	

12. SEGURIDAD EN LA OPERATIVA 12.1 Responsabilidades y procedimientos de operación 12.2 Protección contra código malicioso			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
		permita el seguimiento y monitoreo para llevar a cabo esta tarea periódicamente.	

Tabla 1 - 7 Seguridad en la operativa

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 14.2 Seguridad en los procesos de desarrollo y soporte 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
Incluir una cláusula en el contrato en la cual se defina la metodología y el procedimiento a seguir en el desarrollo del sistema de acreencias y los sistemas de información que se van a utilizar en el periodo de liquidación.	De acuerdo con lo informado por el Ingeniero de Sistemas de la EPS en liquidación, desde el 16 de agosto de 2020 iniciaron el desarrollo del nuevo sistema de información de acreencias, que permitirá llevar a cabo la calificación y graduación de las mismas.		

	Para llevar a cabo este nuevo sistema de información de acreencias, se definió un grupo de trabajo interdisciplinario conformado por un desarrollador contratado de tiempo completo y se encuentra en la las oficinas EPS en Liquidación. Para el desarrollo de esta aplicación el equipo de desarrollo está trabajando bajo la metodología SCRUM. Con esta metodología se lleva un trabajo en conjunto puesto que existe una interacción en tiempo real. De acuerdo a lo indagado, la EPS en liquidación tiene presupuestado para el primero de octubre de 2020 empezar a trabajar con el nuevo sistema de información de acreencias, inicialmente con el tema de prestaciones económicas.		
Diseño, desarrollo, implementación y monitoreo de set de pruebas y casos de usos para determinar el resultado de las pruebas y la satisfacción por parte de los usuarios de la EPS en liquidación, los cuales deben quedar totalmente	En la actualidad el nuevo sistema de información de acreencias se encuentra en etapa de desarrollo, existe un prototipo del sistema de información, asimismo se puede ver parte de la funcionalidad en la siguiente URL	Previó a la instalación en producción de la nueva solución (sistema de información de acreencias), realizar y documentar las pruebas técnicas y funcionales	

documentados.	10.99.211.xxx/iuAcreenciaAud/#/, la cual está en un ambiente de pruebas. Disponen de unas actas de reunión que llevan a cabo donde revisan el estado de avance del aplicativo de acreencias, además, llevan un reporte de actividades del proceso de acreencias diario, en este se evidencia la hora de inicio, la hora fin, el funcionario, el proyecto, tipo de tarea, detalle de la tarea, entre otros.	efectuadas, así como, dejar evidencia de aceptación por parte de los líderes de los procesos inherentes en la EPS en Liquidación.	
Para futuras capacitaciones se debe tener un mecanismo de medición de la misma donde se evalué el aprendizaje, el facilitador y el resultado de la asimilación del conocimiento en el aprovechamiento y uso del sistema.	Actualmente vienen realizando capacitaciones a los operadores sobre el manejo del nuevo sistema de información de acreencias.	Evidenciar la ejecución del proceso de capacitación para todos los funcionarios de La EPS en liquidación.	

Tabla 1 - 8 Adquisición, desarrollo y mantenimiento de los sistemas de información

11. SEGURIDAD FÍSICA Y AMBIENTAL. • **11.1 Áreas seguras** • **11.2 Seguridad de los equipos**			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
Ubicar el centro de comunicaciones en un sitio seguro y restringido y es necesario que se reciba a satisfacción el cableado y con la respectiva certificación.	Se pudo evidenciar que el centro de comunicaciones de la EPS en liquidación se encuentra en lugar razonablemente seguro.		

Tabla 1 - 9 Seguridad física ambiental.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. • **17.1 Continuidad de la seguridad de la información.** • **17.2 Redundancias.**			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
Incluir una política con la cual se garantice, la continuidad del procesamiento de la información en un sitio alterno al centro de cómputo en caso de presente fallas en el centro de cómputo principal de la EPS en Liquidacion.	No existe una Politica que considere la continuidad del procesamiento de la información en un sitio alterno al centro de cómputo.	Definir como garantizar la continuidad del procesamiento de la información en un sitio alterno al centro de cómputo en caso de presente indisponibilidad del centro de cómputo principal o de algunos de sus componentes claves	

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. • **17.1 Continuidad de la seguridad de la información.** • **17.2 Redundancias.**			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
Debido a que en la EPS en liquidación no se tiene un plan de contingencia se recomienda una vez identificados los procesos, aplicaciones y sistemas que continuarán en funcionamiento, elaborar un instructivo de recuperación oportuno, actualizado y suficientemente probado, que permita garantizar la continuidad del procesamiento de información.	Actualmente la EPS en liquidación no dispone de un plan de contingencia.	Implementación del plan de contingencia; este plan debe ser oportuno, actualizado y suficientemente probado para garantizar la continuidad del procesamiento de información de la EPS en Liquidación. Definir y establecer un cronograma para realizar las diferentes pruebas al plan de continuidad. Las pruebas, su resultado y acciones que se deriven de las mismas deben quedar documentadas formalmente. Diseñar un plan de capacitación para los funcionarios, con el fin de que conozcan los procedimientos, controles y acciones a seguir en caso de activarse una contingencia	

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. • **17.1 Continuidad de la seguridad de la información.** • **17.2 Redundancias.**			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
		mayor debida a fallas técnicas o desastres naturales o provocados.	

Tabla 1 - 10 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. **16.1 Gestión de incidentes de seguridad de la información y mejoras.** • **16.1.2 Notificación de los eventos de seguridad de la información.** • **16.1.3 Notificación de puntos débiles de la seguridad.** • **16.1.5 Respuesta a los incidentes de seguridad.**			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
A nivel interno implementar una herramienta de software libre para la gestión de atención de incidentes.	La EPS en liquidación tiene implementada una mesa de ayuda (GLPI) que le permite llevar la gestión de incidentes que puedan ocurrir dentro de la institución, además, disponen de un correo electrónico donde los usuarios puede solicitar ayuda en caso de tener un incidente. Según lo informado por Ingeniero de Sistemas, realizaron la		

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. 16.1 Gestión de incidentes de seguridad de la información y mejoras. • 16.1.2 Notificación de los eventos de seguridad de la información. • 16.1.3 Notificación de puntos débiles de la seguridad. • 16.1.5 Respuesta a los incidentes de seguridad.			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
	capacitación a todos los funcionarios de la entidad en el manejo de esta herramienta de gestión de incidentes.		

Tabla 1 - 11 Gestión de incidentes en la seguridad de la información.

12. SEGURIDAD EN LA OPERATIVA. • 12.3 Copias de seguridad.			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
Incluir una política de acceso, monitoreo y seguimiento al sitio de almacenamiento externo.	Realizar una política para el permiso de acceso y monitoreo ´para el almacenamiento externo.		
Se carece de procedimientos formales periódicos de restauración de backups, que incluyan bases de datos con información crítica o sensible.	El Ingeniero informó que en la actualidad disponen de procedimientos de administración y restauración de backups, en este no se evidencia la periodicidad con la que realizan las restauraciones.	Implementar procedimiento de restauración periódico de Backups. Se sugiere esta prueba se ejecute al menos cada tres meses seleccionando	

12. SEGURIDAD EN LA OPERATIVA. • **12.3 Copias de seguridad.**			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
	No se pudo evidenciar si lo transcurrido del año se han hecho pruebas de restauración de información.	aleatoriamente información crítica y documentando los resultados.	

Tabla 1 - 12 Seguridad en la operativa.

8. GESTIÓN DE ACTIVOS. • **8.2 Clasificación de la información.** • **8.3 Manejo de los soportes de almacenamiento.**			
Recomendación	**Seguimiento**	**Nuevo compromiso**	**Evaluación de seguimiento**
Incluir un politica de las licencias de los servidores.	Se encuentra una politica donde se registra los Servicios **de infraestructura de cómputo**, donde se encuentra estipulado la administración de las licencias de los servidores.		

Tabla 1 - 13 Gestión de activos.

7.4. ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN

Tanto los servidores, como la información que éstos procesan, son un factor crítico para la capacidad de muchas organizaciones de realizar su misión y las funciones del negocio.

Por ello resulta necesario diseñar e implementar un esquema de seguridad de la información, el cual debe estar compuesto como mínimo de tres elementos:

1. Políticas de seguridad que establezcan normas y mecanismos a cumplir y utilizar para proteger la información de la organización, y que a su vez, proporcionen criterios para auditar los mismos.

2. Controles y mecanismos de seguridad física, dentro y alrededor del centro de cómputo, cuyo fin sea la protección tanto del hardware como del software de almacenamiento de datos.

3. Planes de contingencia que garanticen la continuidad de los negocios al momento de ocurrir un desastre o incidente.

Para revisar este esquema revisamos los siguientes pasos :

Las vulnerabilidades las cuales fueron identificadas, luego de realizar el pentesting con las cuales identificamos 70 vulnerabilidades las cuales estaban en un nivel alto, medio, y bajo entre las de alto y bajo tuvimos un total de 58 vulnerabilidades las cuales se repetían algunas en las mismas IP a continuación en el anexo 1 podran encontrar la información de las vulnerabilidades encontradas, el nombre , su descripción , el factor de riesgo, las maquinas afectadas, en que grado de vulnerabilidad se encuentran, los servicios que se están afectando y colocamos una posible solución para mitigar el riesgo de las vulnerabilidades recomendamos realizar cuanto antes un plan de acción correctiva de nuestras recomendaciones si no sus consecuencias podrían ser catastróficas.
Para gestionar la seguridad de la información revisamos riesgos empezamos por sacar una matriz de criticidad para medir los riesgos posibles partiendo de las vulnerabilidades y las entrevistas que se hicieron al personal de sistemas, se revisó físicamente donde se encuentran los servidores de la EPS en liquidación, manejamos un inventario de lo principal del centro de cómputo, de acá comenzamos a definir los riesgos de seguridad presentes sobre los activos, siendo estos valorados en términos de probabilidad de ocurrencia del riesgo y el nivel de impacto que podría generar para la organización la materialización del riesgo, se identificaron los controles existentes, y se recomendaron algunos controles los cuales fueron implementados de la

ISO2002 el cual mitigo un poco el riesgo.

Se le dio un seguimiento a la recomendación de controles si se estaban cumpliendo o no.
Se realizan las siguientes recomendaciones para tener en cuenta después de la revisión para evitar la materialización de riesgos y evitar vernos afectados por alguna vulnerabilidad.
Realizar pruebas periódicas de vulnerabilidad y de la efectividad del plan de reacción o plan de respuesta a incidentes, revisar el anexo 1 de las vulnerabilidades encontradas y realizar las recomendaciones propuestas.
Se debe mantener actualizado el inventario de activos de información (Sistemas de información, Equipos de Cómputo, Backups, Manual de Políticas y Procedimientos de realización y restauración de Backups,Servicios, Pólizas.
Se deben Diseñar las estrategias y los procedimientos para atender los desastres e incidentes informáticos.

A Corto plazo

Copias de seguridad.
EPS en liquidación dispone de un procedimiento de administración y restauración de backup, pero en este procedimiento no se evidencia la periodicidad con la que realizan las restauraciones de backup.
Recomendación: Se debe realizar y documentar pruebas restauración de Backup con el fin de garantizar la disponibilidad de la información almacenada.
Actualizar el proceso actual de administración y restauración de back up que dispone la entidad, donde se establezca la periodicidad con la cual se van a realizar los back up.

Continuidad del negocio desde tecnología.
Actualmente la EPS en liquidación no tiene un plan de continuidad establecido que permita la protección de la información CORE del negocio.
Recomendación: Implementar un plan de continuidad del negocio que permita proteger los procesos críticos y operativos de la corporación contra desastres bien sea naturales o provocadas, asimismo el plan de continuidad del negocio ayuda a disminuir el impacto en pérdidas de tipo financiero, de información crítica para la organización.
Se recomienda realizar pruebas de restauración con el propósito de establecer el tiempo que conllevaría restablecer el servicio de la entidad.

Desarrollo
Se evidenció que la nueva administración (liquidador) está llevando una buena gestión al tema de graduación y calificación de las acreencias, debido a que están adelantando un nuevo sistema de información que permitirá garantizar que este proceso se lleve a cabo lo más transparente posible y poder dar una parte de tranquilidad a sus acreedores.

Para el nuevo sistema de información de acreencias disponen de un grupo de trabajo de tiempo completo el cual es el encargado de realizar el desarrollo de este, asimismo, la interacción en tiempo real del equipo desarrollador permite observar la necesidad que se tiene y así poder dar solución de manera oportuna, efectiva y eficiente.
Al ingresar al sistema de información de acreencias la contraseña que se solicita al usuario no es robusta, puesto que la única condición que se exige es que sea mínimo de 6 caracteres.
Al momento que un funcionario se le olvide el usuario y/o la contraseña de ingreso al sistema de información, el aplicativo no dispone con la funcionalidad de recuperarla, por lo tanto, el usuario debe comunicarse con el administrador del sistema de información para que le brinde ayuda, lo cual esto incurre en tiempos y atrasos por parte del usuario.
Al realizar el proceso de devolución de las facturas que pertenecen a una acreencia, el sistema de información devuelve todo el trabajo.
Recomendación: Estudiar la posibilidad de implementar en el sistema de información la recuperación tanto de usuario como de la contraseña.
Establecer varios parámetros y características de contraseñas robustas y seguridad al momento de la autenticación en el sistema información de acreencias como:

- ✓ Longitud mínima de 8 caracteres.
- ✓ Inclusión de caracteres especiales.
- ✓ Inclusión de mayúsculas y minúsculas.
- ✓ Exclusión de caracteres consecutivos.
- ✓ Control para caracteres adyacentes.
- ✓ Bloqueo por número de intentos de acceso fallidos.

y/o que cumplan con lo establecido en el estándar de claves de acceso.

En el proceso de devoluciones de facturas que el sistema de información solo realice el envío de las que realmente se van a devolver y no envíe todas las facturas.

Usuarios roles y perfiles

No existe un control por parte de la EPS en liquidación de los usuarios que actualmente se encuentran activos e inactivos en los sistemas de información que dispone la entidad.
Recomendación: Se debe emprender acciones para que la administración de los roles y perfiles esté en cabeza de los líderes de los procesos claves del negocio de la EPS en Liquidación.
Implementar un procedimiento formal de verificación periódica de roles y perfiles de los sistemas de información claves de la EPS en Liquidación. Esta actividad debe ser ejecutada con la participación de los líderes funcionales de los procesos del negocio con el apoyo del área de sistemas de la entidad.
Se debe dejar evidencia documentada de la actividad, el resultado de la misma, las acciones y los responsables de ejecución que se deriven de estas

revisiones.

Mediano Plazo

Internet / Intranet
La entidad no realiza monitoreo y seguimiento sobre la navegación en internet que realiza los funcionarios de la entidad, además existen funcionarios que pueden navegar sin ninguna restricción, con la posibilidad que se filtre algún tipo de virus en la red de la institución.
Recomendación: Solicitar reportes semanales de monitoreo y seguimiento a Internet (mediante indicadores de uso de ancho de banda, acceso a Internet, entre otros), adicionalmente, solicitar una herramienta de seguimiento y monitoreo para llevar a cabo esta tarea periódicamente.

8. CONCLUSIONES

El objetivo fundamental del proyecto de grado era abordar la problemática del esquema de seguridad de la información, basado bajo la norma ISO27001:2013, en entornos virtual izados sobre la herramienta Hyper-V e identificar - evaluar cada uno de los riesgos y vulnerabilidades de cada uno de los servidores implementados en la EPS en liquidación con el fin de que todas las aplicaciones migradas e implementadas se mantenga siempre en los tres pilares de la información la integridad, disponibilidad y confidencialidad para cada uno de los usuarios finales de la entidad.

Los riesgos encontrados en cada una de las maquinas implementadas se entregará a área de TICS con el fin de que mitiguen esas vulnerabilidades y queden con un umbral alto en seguridad y así minimizar en un porcentaje alto de vulnerabilidad tanto interna como externamente de cada una de las aplicaciones alojadas en el cuarto de datos propio de la entidad en liquidación.

Después de realizar las evaluaciones correspondientes y utilizar los métodos ya conocidos y mencionados con anterioridad, se concluye que la eps en liquidación presenta algunos umbrales de riesgo en vulnerabilidades las cuales fueron identificadas, luego de realizar el pentesting, por eso es necesario realizar unos procesos para mitigar estos riesgos y vulnerabilidades encontradas y proceder a dar unas indicaciones para dar un alto nivel de seguridad a lo implementado por la eps en liquidación, a continuación nombramos las recomendaciones que hicimos.

- ✓ Impedir acceso a archivos desde navegador.
- ✓ Desactivar los algoritmos de cifrado débiles
- ✓ Filtrar el tráfico generado por los puertos más vulnerables.
- ✓ Reemplazar certificados SSL vencidos por nuevos.
- ✓ Desactivar páginas predeterminadas dentro de la configuración del servidor.
- ✓ Desactivar protocolos de cifrado SSLv2 y SSLv3 obsoletos, utilizar TLSv1 +.
- ✓ Actualizar versión de PHP
- ✓ Utilizar contraseñas con nivel de seguridad alto, además de cambiarlas periódicamente.
- ✓ Actualización y divulgación de las políticas de Seguridad de la Información.
- ✓ Configurar el servicio NFS para que únicamente permita la conexión de equipos autorizados.
- ✓ Aplicar las actualizaciones publicadas por Microsoft en el boletín de seguridad MS14-066.
- ✓ Aplicar las actualizaciones publicadas por Microsoft en el boletín de seguridad MS15-034.

- ✓ Realizar una migración de los servicios a un sistema operativo con soporte por parte del desarrollador

9. BIBLIOGRAFÍA

SIMAD (19 julio, 2017) Consultoría y proyectos IT / Ventajas de Microsoft Hyper-V para tu empresa Recuperado de:http://www.si-mad.com/ventajas-de-microsoft-hyper-v-para-tu-empresa/

NORMAS ISO - ISO 27001 Seguridad de la Información Recuperado de https://www.normas-iso.com/iso-27001/

27001:2013, S. (28 de 01 de 2015). http://www.pmg-ssi.com. Recuperado de: http://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

LOPEZ JOSE MARIA (06 Enero, 2017) Hyper-V, la máquina virtual de Microsoft Recuperado de: https://hipertextual.com/2017/01/hyper-v-maquina-virtual-microsoft

AREVALO CORDOVILLA FELIPE (2018)Gestión de seguridad en virtualización de servidores Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/88827/7/farevalocTFM122018memoria.pdf

ISO/ IEC 27001 VERSION 2013. (2013). ISO/ IEC 27001 VERSION 2013.BOGOTA: INCONTEC

VANNESA FONTALVO (12 Septiembre, 2009) leyes y normas contra los delitos informáticos Recuperado de: https://es.slideshare.net/ciclovanessafontalvo/ley-1273-de-2009

DATAWARDEN- Protección de Hipervisores Virtuales Recuperado de: http://datawarden.com/new/soluciones/seguridad/seguridad-para-ambientes-virtuales/proteccion-de-hipervisores-virtuales/

NICOLAS POGGI (3 Diciembre 2018) 24 Estadísticas de Seguridad Informática que Importan en el 2019 Recuperado de: https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

LLANOS RUIZ ANDERSON JULIÁN ,MENESES ORTIZ MIGUEL ANDRÉS (2016) Diseño de un protocolo para la detección de vulnerabilidades en los principales servidores de la Superintendencia de Puertos y Transporte Recuperado de: https://repository.ucatolica.edu.co/handle/10983/14013

RODRIGUEZ DANIELA (14 Abril, 2015- Calculo de riesgo en un proyecto Recuperado de: https://prezi.com/efyepbtwocgi/calculo-del-riesgo-de-un-proyecto/

GUERRERO RINCÓN, BRAYAN LEONARDO (2018) Análisis de la relación costo – beneficio en el diseño e Implementación del sistema de gestión de calidad ISO 27001 en la empresa Gfi informática Colombia S.A.S Recuperado de: https://repository.ucatolica.edu.co/handle/10983/23172

ARCILA BONFANTE, LUIS EDUARDO (2019) Recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información Recuperado de: https://repository.ucatolica.edu.co/handle/10983/23388

Informe_Tratamiento_de_Riesgos_MINTIC.doc (26 Diciembre, 2019Plan de tratamiento del riesgo Recuperado de: https://www.mintic.gov.co/portal/604/articles-100251_plan_tratamiento_seguridad_2020.pdf

TORO SÁNCHEZ CRISTIAN GIOVANNY,HERNÁNDEZ VEGA MARIEN (2014) Guía de auditoría para evaluar el aseguramiento de la disponibilidad de la información en un ambiente Cloud Computing IAAS, bajo la Norma ISO 27001 de 2013 Recuperado de: https://repository.ucatolica.edu.co/handle/10983/1751

David A. Franco, J. L. (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos. Información Tecnológica Vol. 23(3), 113-120.

10. ANEXOS

ANEXO 1. Adjunto archivo en Excel del análisis consolidado del proceso de vulnerabilidades.

ANEXO 2. Herramienta de análisis de brecha para ISO 27001:2013

¡Gracias por utilizar nuestra Herramienta de análisis de brecha para ISO 27001:2013!

Esta es la información que usted ingresó:

4.0 Contexto de la organización

4.1 Conocimiento de la organización y su contexto
Q. 1. ¿La organización determina los fines del SGSI?
R. Sí

Q. 2. ¿La organización determina las cuestiones internas y externas que son pertinentes para la finalidad de SGSI?
R. Sí

Q. 3. ¿Determina la organización cómo las cuestiones internas y externas podrían influenciar en la capacidad del SGSI para conseguir los resultados previstos?
R. Sí

4.2 Comprensión de las necesidades y expectativas de las partes interesadas
Q. 4. ¿La organización determina las partes interesadas?
R. Sí

Q. 5. ¿Existe la lista de todos los requisitos de las partes interesadas?
R. No

4.3 Determinar el alcance del SGSI
Q. 6. ¿El alcance está documentado con los límites claramente definidos?
R. Sí

4.4 SISTEMAS DE GESTION DE INFORMACION DE SEGURIDAD
Q. 7. ¿Han establecido, documentado, implementado, mantenido y mejorado continuamente un sistema de gestión de seguridad de información según los

requisitos de la norma ISO 27001?
R. Sí

5.0 Liderazgo

5.1 Liderazgo y compromiso
Q. 8. ¿Los objetivos generales del SGSI son compatibles con la dirección estratégica?
R. Sí

Q. 9. ¿La dirección garantiza los recursos necesarios para el SGSI cuando sea necesario?
R. Sí

Q. 10. ¿La dirección asegura que el SGSI logra sus resultados previstos?
R. Sí

5.2 Política
Q. 11. ¿Existe una política de seguridad de la información con objetivos definidos o un marco para el establecimiento de objetivos?
R. No

Q. 12. ¿La política de seguridad de información está documentada y es comunicada dentro de la empresa y a otras partes interesadas?
R. Sí

5.3 Roles, responsabilidades y autoridades en la organización
Q. 13. ¿Están asignadas y comunicadas los roles, responsabilidades y autoridades para la seguridad de la información?
R. Sí

6.0 Planificación

6.1 Acciones para tratar riesgos y oportunidades

6.1.1 Generalidades
Q. 14. ¿Las cuestiones internas y externas, así como los requisitos de las parte sinteresadas, son consideradas al abordar los riesgos y las oportunidades?
R. Sí

6.1.2 Valoración de riesgos de seguridad de la información

Q. 15. ¿Hay un proceso documentado para identificar los riesgos de seguridad de la información, incluyendo los criterios de aceptación del riesgo y criterios de evaluación del riesgo?
R. Sí

6.1.3 Tratamiento de riesgos de la seguridad de la información
Q. 16. ¿Está documentado el proceso de tratamiento del riesgo, incluyendo la sopciones de tratamiento del riesgo y cómo crear una declaración de aplicabilidad?
R. Sí

6.2 Objetivos de seguridad de la información y planes para lograrlos
Q. 17. ¿Los objetivos de seguridad de la información son establecidos en las funciones relevantes de la organización, medido en su práctica y coherente con la política de seguridad de la información?
R. No

Q. 18. ¿Existe un plan, o conjunto de planes, para lograr los objetivos de seguridad de la información incluyendo responsabilidades, método de evaluación y tiempos para el plan?
R. Sí

7.0 Soporte

7.1 Recursos
Q. 19. ¿Se proporcionan los recursos adecuados para todos los elementos del SGSI?
R. Sí

7.2 Competencia
Q. 20. ¿Es evaluada la competencia, y la capacitación donde sea necesario, para el personal que realiza tareas que puedan afectar a la seguridad de la información? ¿Los registros de competencias son mantenidos?
R. Sí

7.3 Concienciación
Q. 21. ¿El personal es consciente de la política de seguridad de la información, de su papel y las consecuencias de no cumplir con las normas?
R. Sí

7.4 Comunicación
Q. 22. ¿Hay un proceso de comunicación relacionado con la seguridad de la información, incluyendo las responsabilidades, qué se comunica, a quién y cuándo?
R. No

7.5 Información documentada (7.5.1 General; 7.5.2 Creación y actualización; 7.5.3 Control de información documentada)
Q. 23. ¿La documentación del SGSI incluye la política de seguridad de la información, objetivos, el alcance del SGSI, los principales elementos y su interacción, documentos y registros de la norma ISO 27001 y aquellos identificados por la empresa?
R. Sí

Q. 24. ¿Se asegura que existe un manejo de documentos y registros, incluyendo quién revisa y aprueba los documentos, cómo y dónde se publican, almacenan y protegen?
R. Sí

Q. 25. ¿Es controlada la información documentada de origen externo?
R. Sí

8.0 Operación

8.1 Planificación y control operacional
Q. 26. ¿La organización tiene la información documentada necesaria para estar segura de que sus procesos se llevan a cabo según lo planeado?
R. Sí

Q. 27. ¿Se controlan los cambios planificados? ¿Las consecuencias de cambios no planificados son revisados para identificar acciones de mitigación?
R. Sí

Q. 28. ¿Los procesos tercerizados son identificados y controlados?
R. Sí

8.2 Apreciación de los riesgos de seguridad de información
Q. 29. ¿Los riesgos, sus propietarios, la probabilidad, las consecuencias y el nivel de riesgo son identificado? ¿Estos resultados se encuentran documentados?
R. Sí

8.3 Tratamiento de los riesgos de seguridad de información
Q. 30. ¿Existe un plan de tratamiento del riesgo, aprobado por los propietarios de riesgo?
R. Sí

Q. 31. ¿Hay una lista documentada con todos los controles necesarios, con el estado aplicación y justificación?
R. Sí

9.0 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación
Q. 32. ¿Está definido qué tiene que ser medido, a través de qué método, quien es responsable, y quien analizará y evaluará los resultados?
R. Sí

Q. 33. ¿Los resultados de medición son documentados, analizados y evaluados por personas responsables?
R. Sí

9.2 Auditoría Interna
Q. 34. ¿Existe un programa de auditoría que define las fechas, responsabilidades, reportes, criterios de auditoría y alcance?
R. No

Q. 35. ¿Las auditorías internas son realizadas según un programa de auditoría, los resultados se informan a través de un informe de auditoría interna y se levantan o identifican acciones correctivas?
R. Sí

9.3 Revisión por la dirección
Q. 36. ¿La Revisión por dirección se realizada regularmente, y se documentan los resultados en actas de reunión?
R. Sí

Q. 37. ¿La dirección decide sobre todas las cuestiones cruciales importantes para el éxito del SGSI?
R. Sí

10.0 Mejora

10.1 No conformidad y acciones correctivas
Q. 38. ¿La organización reacciona a cada no conformidad?
R. Sí

Q. 39. ¿La organización considera la eliminación de la causa de la no conformidad y,en su caso, toma medidas correctivas?
R. Sí

Q. 40. ¿Se registran todas las no conformidades, junto con las acciones correctivas?
R. No

10.2 Mejora continua
Q. 41. ¿El SGSI se ajusta continuamente para mantener su idoneidad, adecuación y eficacia?
R. Sí

R. 88.89

R. - Anexo A. (Nota: Deben ser implementados sólo los controles marcados como aplicable en la Declaración de Aplicabilidad.)

R. - A.5 Políticas de seguridad

A.5 Políticas de seguridad
Q. 42. ¿Existen políticas publicadas, aprobadas por la dirección, para apoyar la seguridad de la información?
R. Sí

Q. 43. ¿Las políticas de seguridad de la información son revisadas y actualizadas?
R. Sí

R. - A.6 Organización de la seguridad

A.6 Organización de la seguridad
Q. 44. ¿Están definidas todas las responsabilidades de seguridad de la información?
R. No

Q. 45. ¿Los deberes y las responsabilidades son correctamente segregadas teniendo en cuenta las situaciones de conflicto de intereses?
R.

Q. 46. ¿Existen definidas contactos con las autoridades competentes?

R. No

Q. 47. ¿Existen definidos contactos con grupos de interés especial o asociaciones profesionales?
R. No

Q. 48. ¿Los proyectos consideran aspectos relacionados con la seguridad de la informacion?
R. No

Q. 49. ¿Existen definidas reglas para el manejo seguro de los dispositivos móviles?
R. No

Q. 50. ¿Existen reglas que definen cómo está protegida la información de la organización teniendo en cuenta el teletrabajo?
R. Sí

R. - A.7 Seguridad relativa a los recursos humanos

A.7 Seguridad relativa a los recursos humanos
Q. 51. ¿La organización realiza verificaciones de antecedentes de los candidatos para el empleo o para los contratistas?
R. Sí

Q. 52. ¿Existen acuerdos con los empleados y contratistas donde se especifiquen las responsabilidades de seguridad de información?
R. No

Q. 53. ¿La dirección requiere activamente que todos los empleados y contratistas cumplan con las reglas de seguridad de la información?
R. - Sí

Q. 54. ¿Los empleados y contratistas asisten a entrenamientos para realizar mejor sus tareas de seguridad, y existen programas de sensibilización?
R. No

Q. 55. ¿La organización tiene un proceso disciplinario?
R. No

Q. 56. ¿Existen acuerdos que cubren las responsabilidades de seguridad de información que siguen siendo válidas después de la terminación del empleo?
R. Sí

R. - A.8 Gestión de activos

A.8 Gestión de activos
Q. 57. ¿Existe un inventario de activos?
R. Sí

Q. 58. ¿Todos los activos en el inventario de activos tienen un dueño designado?
R. Sí

Q. 59. ¿Existen definidas reglas para el manejo de activos y de información?
R. Sí

Q. 60. ¿Los activos de la organización son devueltos cuando los empleados y contratistas finalizan su contrato?
R. Sí

Q. 61. ¿Están definidos los criterios para clasificar la información?
R.

Q. 62. ¿Existen procedimientos que definen cómo etiquetar y manejar información clasificada?
R. Sí

Q. 63. ¿Existen procedimientos que definen cómo manejar activos?
R. Sí

Q. 64. ¿Existen procedimientos que definen cómo manejar medios extraíbles en consonancia con las reglas de clasificación?
R.

Q. 65. ¿Existen procedimientos formales para la eliminación de medios?
R. Sí

Q. 66. ¿Son protegidos los medios que contienen información sensible durante el transporte?
R. Sí

R. - A.9 Control de acceso

A.9 Control de acceso
Q. 67. ¿Existe una política de control de acceso?
R. Sí

Q. 68. ¿Los usuarios tienen acceso sólo a los recursos que se les permite?
R. Sí

Q. 69. ¿Los derechos de acceso son proporcionados mediante un proceso de registro formal?
R. Sí

Q. 70. ¿Existe un sistema de control de acceso formal para el inicio de sesión en sistemas de información?
R. Sí

Q. 71. ¿Los derechos de acceso privilegiado son manejados con especial cuidado?
R. Sí

Q. 72. ¿Las contraseñas, y otra información de autenticación secreta, es proporcionada de forma segura?
R. Sí

Q. 73. ¿Los propietarios de activos comprueban periódicamente todos los derechos de acceso privilegiado?
R. No

Q. 74. ¿Los derechos de acceso son actualizados cuando hay un cambio en la situación del usuario (por ejemplo: cambio organizacional o terminación)?
R. No

Q. 75. ¿Existen reglas para los usuarios sobre cómo proteger las contraseñas y otra información de autenticación?
R. No

Q. 76. ¿El acceso a la información en los sistemas es restringido según la política de control de acceso?
R. Sí

Q. 77. ¿Es requerido un sistema de login en los sistemas según la política de control de acceso?
R. Sí

Q. 78. ¿Los sistemas de gestión de contraseñas utilizados por los usuarios de la organización les ayuda a manejar de forma segura su información de autenticación?
R. Sí

Q. 79. ¿El uso de herramientas de utilidad es controlado y limitado a empleados específicos?
R. Sí

Q. 80. ¿El acceso al código fuente es restringido a personas autorizadas?

R. Sí

R. - A.10 Criptografía

A.10 Criptografía
Q. 81. ¿Existe una política para regular la encriptación y existen otros controles criptográficos?
R. Sí

Q. 82. ¿Están debidamente protegidas las claves criptográficas?
R. Sí

R. - A.11 Seguridad física y del entorno

A.11 Seguridad física y del entorno
Q. 83. ¿Existen zonas seguras que protegen la información sensible?
R. Sí

Q. 84. ¿Es protegida la entrada a las zonas seguras?
R. Sí

Q. 85. ¿Las zonas seguras están ubicadas en un lugar protegido?
R. Sí

Q. 86. ¿Existen instaladas alarmas, sistemas de protección contra incendios y otros sistemas?
R. Sí

Q. 87. ¿Existen definidos procedimientos para las zonas seguras?
R. Sí

Q. 88. ¿Las zonas entrega y carga están protegidas?
R. Sí

Q. 89. ¿Los equipos son debidamente protegidos?
R. Sí

Q. 90. ¿Los equipos están protegidos contra las variaciones de energía?
R. Sí

Q. 91. ¿Están adecuadamente protegidos los cables de energía y telecomunicaciones?
R. Sí

Q. 92. ¿Existe mantenimiento de los equipos?
R. Sí

Q. 93. ¿La retirada de información y equipos fuera de la organización está controlada?
R. Sí

Q. 94. ¿Los activos de la organización son debidamente protegidos cuando no están en las instalaciones de la organización?
R. Sí

Q. 95. ¿Es correctamente eliminada la informacion de los equipos que se van a eliminar?
R. No

Q. 96. ¿Existen reglas para proteger los equipos cuando estos no estén siendo usados por los usuarios?
R. Sí

Q. 97. ¿Hay orientaciones a los usuarios sobre qué hacer cuando estos no están presentes en sus estaciones de trabajo?
R. Sí

R. - A.12 Seguridad de las operaciones

A.12 Seguridad de las operaciones
Q. 98. ¿Estan documentados los procedimientos de TI?
R. Sí

Q. 99. ¿Los cambios que podrían afectar a la seguridad de la información son estrictamente controlados?
R. Sí

Q. 100. ¿Los recursos son monitoreados y se realizan planes para asegurar su capacidad para cumplir con la demanda de los usuarios?
R. Sí

Q. 101. ¿Se separan los entornos de desarrollo, pruebas y producción?
R. Sí

Q. 102. ¿El software antivirus y otros programas para la protección de malware se instalan y utilizan correctamente?
R. Sí

Q. 103. ¿Existe una política de backup definida y se lleva a cabo correctamente?
R. Sí

Q. 104. ¿Los eventos relevantes de lo sistemas son verificando periodicamente?
R. Sí

Q. 105. ¿Los registros están protegidos adecuadamente?
R. Sí

Q. 106. ¿Estan adecuadamente protegidos los logs de los administradores?
R. Sí

Q. 107. ¿Esta la hora de todos los sistemas de TI sincronizada?
R. Sí

Q. 108. ¿La instalación de software es estrictamente controlada?
R. Sí

Q. 109. ¿La información de análisis de vulnerabilidades es correctamente gestionada?
R. Sí

Q. 110. ¿Existen reglas para definir restricciones de instalación de software a los usuarios?
R. Sí

Q. 111. ¿Estan las auditorías de sistemas de producción planeadas y se ejecutan correctamente?
R. No

R. - A.13 Seguridad de las comunicaciones

A.13 Seguridad de las comunicaciones
Q. 112. ¿Las redes son gestionadas para proteger la información de sistemas y aplicaciones?
R. Sí

Q. 113. ¿Los requisitos de seguridad para servicios de red están incluidas en los acuerdos?
R. Sí

Q. 114. ¿Existen redes segregadas considerando los riesgos y la clasificacion de los activos?
R. Sí

Q. 115. ¿Las transferencias de información están debidamente protegidas?
R. Sí

Q. 116. ¿Los acuerdos con terceras partes consideran la seguridad durante la transferencia de información?
R. Sí

Q. 117. ¿Los mensajes que se intercambian sobre las redes están protegidos correctamente?
R. Sí

Q. 118. ¿La organización posee una lista xon todas las cláusulas de confidencialidad que deben ser incluidos en los acuerdos con terceros?
R. No

R. - A.14 Adquisición, desarrollo y mantenimiento de sistemas de información

A.14 Adquisición, desarrollo y mantenimiento de sistemas de información
Q. 119. ¿Se definen requisitos de seguridad para nuevos sistemas de información, o para cualquier cambio sobre ellos?
R. Sí

Q. 120. ¿La información de aplicaciones transferida a través de redes públicas es adecuadamente protegida?
R. Sí

Q. 121. ¿Las transacciones de información a través de redes públicas son adecuadamente protegidas?
R. Sí

Q. 122. ¿Existen definidas reglas para el desarrollo seguro de software y de los sistemas?
R. Sí

Q. 123. ¿Se controlan los cambios en los sistemas nuevos o existentes?
R. Sí

Q. 124. ¿Las aplicaciones criticas son debidamente probadas después de los cambios realizados en los sistemas operativos?
R. Sí

Q. 125. ¿Se realizan sólo los cambios necesarios a los sistemas de información?
R. Sí

Q. 126. ¿Los principios de ingeniería de sistemas seguros son aplicados al proceso de desarrollo de sistemas de la organización?
R. Sí

Q. 127. ¿Es seguro el entorno de desarrollo?
R. Sí

Q. 128. ¿Es monitorizado el desalloro externalizado de sistemas?
R. Sí

Q. 130. ¿Existe definido un criterio para aceptar los sistemas?
R. Sí

Q. 131. ¿Los datos de prueba son cuidadosamente seleccionados y protegidos?
R. Sí

R. - A.15 Relación con proveedores

A.15 Relación con proveedores
Q. 132. ¿Existe una política para el tratamiento de los riesgos relacionados con proveedores y socios?
R. No

Q. 133. ¿Los requisitos de seguridad son incluidos en los acuerdos con los proveedores y socios?
R. No

Q. 134. ¿Los acuerdos con los proveedores incluyen requisitos de seguridad?
R. No

Q. 135. ¿Son supervisados regularmente los proveedores?
R. No

Q. 136. ¿Los cambios relacionados con los acuerdos y contratos con proveedores y socios tienen en cuenta los riesgos existentes?
R. No

R. - A.16 Gestión de incidentes de seguridad de la información

A.16 Gestión de incidentes de seguridad de la información
Q. 137. ¿Los incidentes son gestionados adecuadamente?
R. Sí

Q. 138. ¿Los eventos de seguridad son reportados adecuadamente?
R. Sí

Q. 139. ¿Los empleados y contratistas informan sobre las debilidades de

seguridad?
R. No

Q. 140. ¿Los eventos de seguridad son evaluados y clasificados correctamente?
R. Sí

Q. 141. ¿Están documentados los procedimientos para dar respuesta a los incidentes?
R. Sí

Q. 142. ¿Se analizan los incidentes de seguridad correctamente?
R. Sí

Q. 143. ¿Existen procedimientos que definen cómo recopilar evidencias?
R. Sí

R. - A.17.Aspectos de seguridad de la información para la gestión de la continuidad del negocio

A.17.Aspectos de seguridad de la información para la gestión de la continuidad del negocio
Q. 144. ¿Existen definidos requisitos para la continuidad de la seguridad de la información?
R. Sí

Q. 145. ¿Existen procedimientos que aseguren la continuidad de la seguridad de la información durante una crisis o un desastre?
R. Sí

Q. 146. ¿Se realizan tests y pruebas de continuidad?
R. Sí

Q. 147. ¿La infraestructura IT está redundada, incluyendo su planeamiento y operación?
R. Sí

R. - A.18 Cumplimiento

A.18 Cumplimiento
Q. 148. ¿Son conocidos los requisitos legislativos, regulatorios, contractuales y cualquier otro requisito relativo a seguridad?
R. Sí

Q. 149. ¿Existen procedimientos para proteger los derechos de propiedad intelectual?

R. No

Q. 150. ¿Los registros están protegidos adecuadamente?
R. Sí

Q. 151. ¿La informacion personal está protegida adecuadamente?
R. Sí

Q. 152. ¿Se utilizan controles criptográficos correctamente?
R. Sí

Q. 153. ¿La seguridad de la información es revisada regularmente por un auditor independiente?
R. No

Q. 154. ¿Los gerentes revisan regularmente si las políticas de seguridad y procedimientos son llevados a cabo adecuadamente en sus áreas de responsabilidad?
R. Sí

Q. 155. ¿Los sistemas de información son revisados regularmente para comprobar su cumplimiento con los estándares y las políticas de seguridad de la información?
R. Sí

Q. Cantidad de controles cumplimentados:
R. 88